(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 215 905 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
17.05.2006 Bulletin 2006/20

(51) Int Cl.:
H04N 7/167 (2006.01) *H04N 5/913* (2006.01)
H04H 1/00 (2006.01) *H04L 9/08* (2006.01)
H04L 9/00 (2006.01)

(21) Application number: **01310230.6**

(22) Date of filing: **06.12.2001**

(54) **Reception apparatus having a storage unit for recording a scrambled broadcast signal and broadcast apparatus for scrambling a signal to be broadcast, and associated methods**

Empfangsgerät mit Aufzeichnungseinheit zum Aufzeichnen eines verschlüsselten Rundfunksignals und Rundfunkvorrichtung zum Verschlüsseln eines auszustrahlenden Signals sowie zugehörige Verfahren

Appareil de réception avec unité d'enregistrement pour enregistrer un signal de radiodiffusion brouillé et appareil de radiodiffusion pour brouiller un signal à diffuser, et procédés associés

(84) Designated Contracting States:
DE FR GB

(30) Priority: **15.12.2000 JP 2000381870**

(43) Date of publication of application:
19.06.2002 Bulletin 2002/25

(73) Proprietor: **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**
Kadoma-shi, Osaka 571 (JP)

(72) Inventors:
- **Fukami, Yukiyasu**
  Nagoya-shi,
  Aichi-ken 462-0042 (JP)
- **Nakahara, Toru**
  Osaka-shi,
  Osaka-fu 532-0022 (JP)
- **Matsuo, Takashi**
  Kawasaki-shi,
  Kanagawa-ken 216-0005 (JP)
- **Higashi, Akio**
  Takatsuki-shi,
  Osaka-fu 569-1022 (JP)
- **Murakami, Hiroki**
  Osaka-fu 565-0862 (JP)

(74) Representative: **Butcher, Ian James et al**
A.A. Thornton & Co.
235 High Holborn
London WC1V 7LE (GB)

(56) References cited:
EP-A- 0 903 886
US-A- 5 420 866
US-A- 6 148 082

Printed by Jouve, 75001 PARIS (FR)

EP 1 215 905 B1

Description

BACKGROUND OF THE INVENTION

(1) Field of the Invention

[0001] The present invention relates to a storage service in the digital broadcast or the like, whereby received scrambled content is stored and then descrambled as required. More specifically, the present invention relates to technology for improving performance of the service in some particular reproduction modes.

(2) Description of the Related Art

[0002] In the current pay satellite digital broadcast system, a viewer contracts with a broadcast provider to pay some amount of charges to the broadcast provider for viewing programs on selected channels.

[0003] Since a broadcasting satellite broadcasts on a number of channels, programs on the channels for which a viewer does not make subscribing contracts are also broadcast to the viewer. The receiver owned by the viewer, then, confirms the presence/absence of the subscribing contract for each channel and receives only programs on the channels allowed to be viewed. Such technology for selecting channels to receive programs thereon is called Conditional Access (abbreviated as "CA").

[0004] On the other hand, the transmitter scrambles content including audio and visual data of a pay broadcast program to be broadcast one each channel, where content per predetermined unit is scrambled with a scrambling key different for each predetermined unit of contents. The transmitter, then, sequentially transmits the scrambled content accompanied with an Entitlement Control Message (ECM) containing this scrambling key and the scrambling key for content in the successive predetermined unit. This ECM is encrypted so as to be interpreted only by the receivers owned by subscribers to the channel.

[0005] Note that the scrambling key used for scrambling data functions as a descrambling key as well for descrambling the data.

[0006] Each receiver comes with an IC card used for the receiver only, to which an identifying number associated with the subscriber is assigned. The IC card has a CPU and a memory within it to store contract conditions and software for executing CA processes. The data relating to the CA processes is completely digitized and contained in the IC card, which makes unauthorized viewing difficult and therefore provides high levels of security.

[0007] Meanwhile, the service called a "storage service" is scheduled to become operational targeted for those who have not yet subscribed to a channel so that, once storing scrambled content with ECM in the recording media in the receivers owned by them, they pay some amount of charges for viewing the content to become subscribers, which enables them to decode the ECMs so as to reproduce the stored scrambled content.

[0008] In such a service, when reproducing content in the normal reproduction mode, the receiver acquires content in the first predetermined unit, and decodes the accompanied ECM to extract the scrambling keys for content in the first and the second units. Then, the receiver descrambles the content in the first unit using the scrambling key exclusive to the content. As for the content in the second unit or later, the receiver sequentially descrambles content in each unit using the scrambling key obtained in the process for the preceding unit.

[0009] However, when reproducing content by the storage service in the particular reproduction modes such as a fast-forward reproduction mode and a fast-reverse reproduction mode, the receiver cannot descramble content in each unit using the scrambling key obtained in the process for the preceding unit, because the order of the reproduction becomes different from that in the normal reproduction mode. Therefore, the receiver has to, each time acquiring content in a predetermined unit, decode the accompanied ECM to obtain a scrambling key and descramble the scrambled content using the key, which makes it difficult to realize a sufficient performance level of the particular reproduction modes, such as fast-forward speed.

[0010] For other relevant background information attention is directed to EP-A-0 903 886 A and US-A-6 148 082.

SUMMARY OF THE INVENTION

[0011] The object of the invention is to provide a broadcast apparatus for offering a storage service, a method and a computer program for the same, a reception apparatus for offering the storage service, and a method and a computer program for the same, all of which improve performance of particular reproduction processes in the storage service.

[0012] The reception apparatus (hereafter called "reception apparatus A") for providing a storage service according to the invention is made up of: a reception unit for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content is embedded; a storage unit for storing the received scrambled content and the storage information; a list extraction unit for extracting the list from the stored storage information; a descramble processing unit for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list, and (c) descrambling the

extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction unit for reproducing the predetermined unit of descrambled content in the descrambled order.

[0013] With this construction, the storage information in which the list of the descrambling keys is embedded and the scrambled content can be received and stored. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling scrambled content in the predetermined unit can be extracted from the list.

[0014] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0015] In the above reception apparatus, the reception unit receives one piece of storage information in which the list is embedded, the storage unit stores the received scrambled content and the one piece of storage information, and the list extraction unit extracts the list from the stored one piece of storage information.

[0016] With this construction, the reception apparatus can receive and store a piece of storage information in which the list of descrambling keys is embedded and extract the list from the stored one piece of storage information.

[0017] In the above reception apparatus, the reception unit receives a plurality of pieces of storage information in each piece of which a divided portion of the list is embedded, the storage unit stores the received scrambled content and the plurality of pieces of storage information, and the list extraction unit extracts the list from the stored plurality of pieces of storage information.

[0018] With this construction, the reception apparatus can receive and store the plurality of pieces of storage ECM, in each piece of which a divided portion of the list of descrambling keys is embedded, and extract the list from the stored plurality of pieces of storage information.

[0019] In the above reception apparatus, the reception unit sequentially receives a transport stream (TS) packet including the predetermined unit of scrambled content, the storage unit sequentially stores the received TS packet, wherein the descramble processing unit includes: a scrambled content extraction unit for extracting the predetermined unit of scrambled content from one of the TS packets stored in the storage unit, and counting the ordinal position of the TS packet from the leading TS packet; a descrambling key extraction unit for extracting a descrambling key from the list, based on the counted ordinal position; and a descrambling unit for descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

[0020] With this construction, the reception apparatus counts the number of TS packets from the leading TS packet, and can easily extract a descrambling key from the list, based on the counted number of TS packets.

[0021] In the above reception apparatus A, the reception unit receives at least one storage Entitlement Control Message (ECM) as the at least one piece of storage information, the list being embedded in a portion to be encoded in the main body of the ECM, the storage unit stores the received storage ECMs, and the list extraction unit interprets the stored storage ECMs to extract the list (hereafter called "reception apparatus B").

[0022] With this construction, the reception apparatus can receive and store the storage ECM, where the list is embedded in a portion to be encoded in a main body of the ECM, and interpret the stored storage ECM to extract the list. Therefore, the invention can be realized according to the current standard.

[0023] In the above reception apparatus B, the reception unit receives the storage ECMs including identifying information for distinguishing the storage ECMs from another type of ECM.

[0024] With this construction, the storage ECMs can be easily distinguished from another type of ECM, because the storage ECMs include identifying information.

[0025] In the above reception apparatus B, the reception unit receives the storage ECMs at a time.

[0026] With this construction, the storage ECMs can be transmitted at a time. As a result, a load necessary to control the transmission timing by the broadcast apparatus can be reduced.

[0027] In the above reception apparatus A, the reception unit sequentially receives a TS packet including (a) the predetermined unit of scrambled content and (b) packet specifying information for specifying an unscrambled TS packet, and the storage unit sequentially stores the received TS packet, wherein the descramble processing unit includes: a scrambled content extraction unit for extracting the predetermined unit of scrambled content and the packet specifying information from one of the TS packets stored in the storage unit; a descrambling key extraction unit for extracting a descrambling key from the list, based on the extracted packet specifying information; and a descrambling unit for descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

[0028] With this construction, the descrambling key can be easily extracted from the list, based on the packet specifying information.

[0029] In the above reception apparatus, the packet specifying information is one of Continuity Counter (CC), the number of TS packets, a cumulative amount of data, a relative reproduction time, and a scrambling key identifier, the scrambled content extraction unit extracts, as the packet specifying information, one of the Continuity Counter (CC), the number of TS packets, the cumulative amount of data, the relative reproduction time, and the scrambling key identifier, and the descrambling key extraction unit performs a predetermined operation to the extracted information as the packet identifying information to generate a descrambling key identifier, and extracts a descrambling key from the list based on the descrambling key identifier.

[0030] With this construction, the descrambling key identifier is generated by performing the predetermined operation to one of the CC, the number of TS packets, the cumulative amount of data, the relative reproduction time, and the scrambling key identifier. As compared with the case where the value of one of the above-stated information is set at the value of the descrambling key identifier, the value of the descrambling key identifier becomes difficult to be analyzed by malicious users, which improves the security. In addition, the above-stated information used in the current standard also can be used, and other information which would lead to increase in the amount of transmitted data does not need to be attached to extract the descrambling key.

[0031] In the above reception apparatus A, the reception unit sequentially receives a TS packet including (a) the predetermined unit of scrambled content and (b) unscrambled I picture information, wherein the I picture information indicates whether the TS packet corresponding to the information consists of a portion of an I picture/an I picture or not, and the storage unit sequentially stores the received TS packet, wherein the descramble processing unit includes: a scrambled content extraction unit for, when performing particular reproduction processes, extracting the predetermined unit of scrambled content and I picture information from one of the TS packets stored in the storage unit; an I picture judgement unit for judging whether the extracted predetermined unit of scrambled content consists of a portion of an I picture/an I picture or not, based on the extracted I picture information; a descrambling key extraction unit for extracting a descrambling key from the list, only when the extracted predetermined unit of scrambled content consists of a portion of an I picture/an I picture; and a descrambling unit for descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

[0032] With this construction, the reception apparatus can reproduce I pictures only. As a result, particular reproduction processes such as fast forward reproduction can be easily conducted.

[0033] The above reception apparatus A further managing contract information and consisting of a security module whose portion does not effectively function if a contract has not been made, and other modules, the reception apparatus is further made up of: a list holding unit for holding the list extracted by the list extraction unit, wherein the list extraction unit and the list holding unit are provided within the security module.

[0034] With this construction, the list can be stored within the security module, which prevents the list from being analyzed by malicious users, and therefore improves the security.

[0035] Another reception apparatus (hereafter called "reception apparatus C") for providing a storage service according to the invention is made up of: a reception unit for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and a descrambling key is attached to each predetermined unit of scrambled content; a storage unit for storing the received scrambled content; a list generation unit for, when/after storing the received scrambled content by the storage unit, generating a list including all descrambling keys to be used for descrambling the scrambled content, based on the descrambling key attached to each predetermined unit of scrambled content; a descramble processing unit for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the extracted predetermined unit of scrambled content from the generated list, and (c) descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction unit for reproducing the predetermined unit of descrambled content in the descrambled order.

[0036] With this construction, the reception apparatus can receive and store the scrambled content, while generating and holding the list of the descrambling keys. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling the predetermined unit of scrambled content can be extracted from the list.

[0037] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0038] In the above reception apparatus C, the reception unit sequentially receives a TS packet including (a) the predetermined unit of scrambled content, and (b) auxiliary information including a descrambling key and information for associating the descrambling key with scrambled content, the storage unit sequentially stores the received TS packet, and the list generation unit generates the list, based on the auxiliary information.

[0039] With this construction, the list can be easily generated based on the auxiliary information.

[0040] In the above reception apparatus, the TS packet includes an ECM, the auxiliary information being embedded in a portion to be encoded in a main body of the ECM, and the list generation unit extracts the auxiliary information embedded in the ECM, and generates the list based on the auxiliary information.

[0041] With this construction, the reception apparatus can receive and store the ECM, where the auxiliary information is embedded in the portion to be encoded in the main body of the ECM, and can interpret the stored ECM to generate the list. As a result, the present invention can be realized according to the current standard.

[0042] A broadcast apparatus (hereafter called "broadcast apparatus A") for providing a storage service according to the invention is made up of: an acquisition unit for acquiring content to be scrambled and a plurality

of descrambling keys; a scramble processing unit for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; an attaching unit for attaching auxiliary information to the predetermined unit of scrambled content, the auxiliary information consisting of (a) information for identifying the scrambled content and (b) a descrambling key corresponding to the content, and used for having the reception apparatus generate a list of the descrambling keys; and a broadcast unit for broadcasting the scrambled content to which the auxiliary information is added.

[0043] With this construction, the auxiliary information used for having the reception apparatus generate the list of the descrambling keys can be attached to the scrambled content. As a result, the reception apparatus can easily generate the list of the descrambling keys.

[0044] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0045] In the above broadcast apparatus A, the attaching unit embeds the auxiliary information in a portion to be encoded in a main body of an ECM and attaches the ECM to the predetermined unit of scrambled content.

[0046] With this construction, the broadcast apparatus can attach the ECM to the scrambled content, where the auxiliary information is embedded in the portion to be encoded in the main body of the ECM. As a result, the present invention can be realized according to the current standard.

[0047] Another broadcast apparatus (hereafter called "broadcast apparatus B") for providing a storage service, according to the invention, is made up of: an acquisition unit for acquiring content to be scrambled and a plurality of descrambling keys; a list generation unit for generating a list of the descrambling keys; an embedding unit for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information; a scramble processing unit for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and a broadcast unit for broadcasting the generated storage information and the scrambled content.

[0048] With this construction, the broadcast apparatus can broadcast the storage information in which the list of the descrambling keys is embedded, together with the scrambled content.

[0049] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0050] In the above broadcast apparatus B, the embedding unit embeds the list in one piece of predetermined information to generate one piece of storage information, and the broadcasting unit broadcasts the generated one piece of information and the scrambled content.

[0051] With this construction, the broadcast apparatus can generate and broadcast a piece of storage information in which the list of all descrambling keys is embedded.

[0052] In the above broadcast apparatus B, the embedding unit embeds a divided portion of the list in each of a plurality of pieces of predetermined information to generate a plurality of pieces of storage information, and the broadcasting unit broadcasts the generated plurality of pieces of storage information and the scrambled content.

[0053] With this construction, the broadcast apparatus can generate and broadcast a plurality of pieces of storage information in each piece of which a divided portion of the list of descrambling keys is embedded.

[0054] In the above broadcast apparatus B, the embedding unit embeds the list in a portion to be encoded in a main body of at least one ECM to generate at least one piece of storage information.

[0055] With this construction, the broadcast apparatus can attach the ECM to the scrambled content, where the list is embedded in the portion to be encoded in the main body of the ECM. As a result, the present invention can be realized according to the current standard.

[0056] In the above broadcast apparatus B, the broadcast unit broadcasts one set of the storage information while all the scrambled content corresponding to the storage information are broadcast once.

[0057] This construction can save the amount of data transmitted.

[0058] A program used for a reception apparatus for providing a storage service according to the invention has the reception apparatus conduct the following steps of: a reception step for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content is embedded; a storage step for storing the received scrambled content and the storage information; a list extraction step for extracting the list from the stored storage information; a descramble processing step for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list, and (c) descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction

step for reproducing the predetermined unit of descrambled content in the descrambled order.

[0059] With this construction, the storage information in which the list of the descrambling keys is embedded and the scrambled content can be received and stored. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling scrambled content in the predetermined unit can be extracted from the list.

[0060] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0061] Another program according to the invention has a reception apparatus for providing a storage service conduct the following steps of: a reception step for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and a descrambling key is attached to each predetermined unit of scrambled content; a storage step for storing the received scrambled content; a list generation step for, when/after storing the received scrambled content in the storage step, generating a list including all descrambling keys to be used for descrambling the scrambled content, based on the descrambling key attached to each predetermined unit of scrambled content; a descramble processing step for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the extracted predetermined unit of scrambled content from the generated list, and (c) descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction step for reproducing the predetermined unit of descrambled content in the descrambled order.

[0062] With this construction, the reception apparatus can receive and store the scrambled content, while generating and holding the list of the descrambling keys. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling the predetermined unit of scrambled content can be extracted from the list.

[0063] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0064] A program used for a broadcast apparatus for providing a storage service according to the invention has the broadcast apparatus conduct the following steps of: an acquisition step for acquiring content to be scrambled and a plurality of descrambling keys; a scramble processing step for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; an attaching step for attaching auxiliary information to the predetermined unit of scrambled content, the auxiliary information consisting of (a) information for identifying the scrambled content and (b) a descrambling key corresponding to the content, and used for having the reception apparatus generate a list of the descrambling keys; and a broadcast step for broadcasting the scrambled content to which the auxiliary information is added.

[0065] With this construction, the auxiliary information used for having the reception apparatus generate the list of the descrambling keys can be attached to the scrambled content. As a result, the reception apparatus can easily generate the list of the descrambling keys.

[0066] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0067] Another program according to the invention has a broadcast apparatus for providing a storage service conduct the following steps of: an acquisition step for acquiring content to be scrambled and a plurality of descrambling keys; a list generation step for generating a list of the descrambling keys; an embedding step for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information; a scramble processing step for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and a broadcast step for broadcasting the generated storage information and the scrambled content.

[0068] With this construction, the broadcast apparatus can broadcast the storage information in which the list of the descrambling keys is embedded, together with the scrambled content.

[0069] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0070] A recording medium, according to the invention, on which a program used for a reception apparatus for providing a storage service is recorded, the program has the reception apparatus conduct the following steps of: a reception step for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content

is embedded; a storage step for storing the received scrambled content and the storage information; a list extraction step for extracting the list from the stored storage information; a descramble processing step for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list, and (c) descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction step for reproducing the predetermined unit of descrambled content in the descrambled order.

[0071] With this construction, the storage information in which the list of the descrambling keys is embedded and the scrambled content can be received and stored. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling scrambled content in the predetermined unit can be extracted from the list.

[0072] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0073] Another recording medium, according to the invention, on which a program used for a reception apparatus for providing a storage service is recorded, the program has the reception apparatus conduct the following steps of: a reception step for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and a descrambling key is attached to each predetermined unit of scrambled content; a storage step for storing the received scrambled content; a list generation step for, when/after storing the received scrambled content in the storage step, generating a list including all descrambling keys to be used for descrambling the scrambled content, based on the descrambling key attached to each predetermined unit of scrambled content; a descramble processing step for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the extracted predetermined unit of scrambled content from the generated list, and (c) descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction step for reproducing the predetermined unit of descrambled content in the descrambled order.

[0074] With this construction, the reception apparatus can receive and store the scrambled content, while generating and holding the list of the descrambling keys. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling the predetermined unit of scrambled content can be extracted from the list.

[0075] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0076] A recording medium, according to the invention, on which a program used for a broadcast apparatus for providing a storage service is recorded, the program has the broadcast apparatus conduct the following steps of: an acquisition step for acquiring content to be scrambled and a plurality of descrambling keys; a scramble processing step for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; an attaching step for attaching auxiliary information to the predetermined unit of scrambled content, the auxiliary information consisting of (a) information for identifying the scrambled content and (b) a descrambling key corresponding to the content, and used for having the reception apparatus generate a list of the descrambling keys; and a broadcast step for broadcasting the scrambled content to which the auxiliary information is added.

[0077] With this construction, the auxiliary information used for having the reception apparatus generate the list of the descrambling keys can be attached to the scrambled content. As a result, the reception apparatus can easily generate the list of the descrambling keys.

[0078] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0079] Another recording medium, according to the invention, on which a program used for a broadcast apparatus for providing a storage service is recorded, the program has the broadcast apparatus conduct the following steps of: an acquisition step for acquiring content to be scrambled and a plurality of descrambling keys; a list generation step for generating a list of the descrambling keys; an embedding step for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information; a scramble processing step for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and a broadcast step for broadcasting the generated storage information and the scrambled content.

[0080] With this construction, the broadcast apparatus can broadcast the storage information in which the list of the descrambling keys is embedded, together with the scrambled content.

[0081] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward

speed, to a sufficient level.

[0082] A recording medium according to the invention on which content to be broadcast to a reception apparatus is recorded, the content are made up of: scrambled content which is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of content, and a storage ECM, wherein a list including all descrambling keys used for descrambling the scrambled content is embedded in a portion to be encoded in a main body of at least one ECM.

[0083] With this construction, the broadcast apparatus can broadcast the ECM, where the list including all descrambling keys is embedded in the portion to be encoded in the main body of the ECM. As a result, the extraction of the descrambling key by the reception apparatus receiving the content can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0084] A method for receiving a storage service according to the invention includes the steps of: a reception step for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content is embedded; a storage step for storing the received scrambled content and the storage information; a list extraction step for extracting the list from the stored storage information; a descramble processing step for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list, and (c) descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction step for reproducing the predetermined unit of descrambled content in the descrambled order.

[0085] With this construction, the storage information in which the list of the descrambling keys is embedded and the scrambled content can be received and stored. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling scrambled content in the predetermined unit can be extracted from the list.

[0086] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0087] Another method for receiving a storage service according to the invention includes the steps of: a reception step for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content, and a descrambling key is attached to each predetermined unit of scrambled content; a storage step for storing the received scrambled content; a list generation step for, when/after storing the received scrambled content in the storage step, generating a list including all descrambling keys to be used for descrambling the scrambled content, based on the descrambling key attached to each predetermined unit of scrambled content; a descramble processing step for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, (b) extracting a descrambling key corresponding to the extracted predetermined unit of scrambled content from the generated list, and (c) descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key; and a reproduction step for reproducing the predetermined unit of descrambled content in the descrambled order.

[0088] With this construction, the reception apparatus can receive and store the scrambled content, while generating and holding the list of the descrambling keys. As a result, when reproducing the stored scrambled content, a descrambling key required for descrambling the predetermined unit of scrambled content can be extracted from the list.

[0089] Therefore, the extraction of the descrambling key can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0090] A method for broadcasting a storage service according to the invention includes the steps of: an acquisition step for acquiring content to be scrambled and a plurality of descrambling keys; a scramble processing step for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; an attaching step for attaching auxiliary information to the predetermined unit of scrambled content, the auxiliary information consisting of (a) information for identifying the scrambled content and (b) a descrambling key corresponding to the content, and used for having the reception apparatus generate a list of the descrambling keys; and a broadcast step for broadcasting the scrambled content to which the auxiliary information is added.

[0091] With this construction, the auxiliary information used for having the reception apparatus generate the list of the descrambling keys can be attached to the scrambled content. As a result, the reception apparatus can easily generate the list of the descrambling keys.

[0092] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance

of particular reproduction processes, such as fast forward speed, to a sufficient level.

[0093] Another method for broadcasting a storage service according to the invention includes the steps of: an acquisition step for acquiring content to be scrambled and a plurality of descrambling keys; a list generation step for generating a list of the descrambling keys; an embedding step for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information; a scramble processing step for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and a broadcast step for broadcasting the generated storage information and the scrambled content. With this construction, the broadcast apparatus can broadcast the storage information in which the list of the descrambling keys is embedded, together with the scrambled content.

[0094] Therefore, the extraction of the descrambling key by the reception apparatus can be executed in a short time and at low load, which improves the performance of particular reproduction processes, such as fast forward speed, to a sufficient level.

BRIEF DESCRIPTION OF THE DRAWINGS

[0095] These and the other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings which illustrate a specific embodiment of the invention.

[0096] In the drawings:

FIG. 1 is the construction of a system for providing a storage service according to the first embodiment of the invention;
FIG. 2 shows one example of the data structure of a scrambling key list descriptor;
FIG. 3 shows one example of the data structure of an ECM for storage;
FIG. 4 shows timing for transmitting the scrambling key list;
FIG. 5 shows the detailed construction of the scrambling process unit 103;
FIG. 6 shows a relation between content and scrambling keys in a transport stream (TS);
FIG. 7 shows the scrambling key list associated with the TS shown in FIG. 6;
FIG. 8 shows the detailed construction of the descrambling process unit 204;
FIG. 9 shows a procedure in the broadcasting process by means of the broadcast apparatus 100 according to the first embodiment of the invention;
FIG. 10 shows a procedure in the scrambling process by means of the scrambling process unit 103 in detail.
FIG. 11 shows a procedure in the reception and storage processes by means of the reception apparatus 200 and the security module 300 according to the first embodiment of the invention;
FIG. 12 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 200 and the security module 300 according to the first embodiment of the invention;
FIG. 13 shows a procedure in the descrambling process by means of the descrambling process unit 204 in detail;
FIG. 14 is a schematic view showing an image stream in the MPEG-2 coding system;
FIG. 15 shows a TS obtained by converting the image stream shown in FIG. 14;
FIG. 16 shows a procedure in the descrambling process in the fast-forward reproduction mode in detail;
FIG. 17 shows a portion of the construction of a system for providing a storage service according to the second embodiment of the invention;
FIG. 18 shows the detailed construction of the descrambling process unit 401;
FIG. 19 shows a portion of the construction of a system for providing a storage service according to the third embodiment of the invention;
FIG. 20 shows the detailed construction of the scrambling process unit 601;
FIG. 21 shows the scrambling key list in the case the value of "CC mod 16" is set at the scrambling key identifier;
FIG. 22 shows the detailed construction of the descrambling process unit 701;
FIG. 23 shows a procedure in the broadcasting process by means of the broadcast apparatus 600 according to the third embodiment of the invention;
FIG. 24 shows a procedure in the scrambling process by means of the scrambling process unit 601 in detail;
FIG. 25 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 700 and the security module 300 according to the third embodiment of the invention;
FIG. 26 shows a procedure in the descrambling process by means of the descrambling process unit 701 in detail;
FIG. 27 shows the construction of a system for providing a storage service according to the fourth embodiment of the invention;
FIG. 28 shows one example of the data structure of the scrambling key list generation descriptor;
FIG. 29 shows one example of the data structure of an ECM for normal reproduction, to which the scrambling key list generation descriptor is added;
FIG. 30 shows the detailed construction of the scrambling process unit 802;
FIG. 31 shows the detailed construction of the de-

scrambling process unit 905;
FIG. 32 shows a procedure in the broadcasting process by means of the broadcast apparatus 800 according to the fourth embodiment of the invention;
FIG. 33 shows a procedure in the scrambling process by means of the scrambling process unit 802 in detail;
FIG. 34 shows a procedure in the reception and storage processes by means of the reception apparatus 900 and the security module 1000 according to the fourth embodiment of the invention;
FIG. 35 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 900 and the security module 1000 according to the fourth embodiment of the invention;
FIG. 36 shows a procedure in the descrambling process by means of the descrambling process unit 905 in detail;
FIG. 37 shows the construction of a system for providing a storage service according to the fifth embodiment of the invention;
FIG. 38 is a schematic diagram showing changes in the scrambling keys and timing for updating ECMs for normal reproduction;
FIG. 39 is a schematic diagram showing changes between an even number key and an odd number key, and timing for updating ECMs for normal reproduction;
FIG. 40 shows a transition of the scrambling key list generated;
FIG. 41 shows the detailed construction of the descrambling process unit 1207;
FIG. 42 shows a procedure in the broadcasting process by means of the broadcast apparatus 1100 according to the fifth embodiment of the invention;
FIG. 43 shows a procedure in the reception and storage processes by means of the reception apparatus 1200 and the security module 1300 according to the fourth embodiment of the invention;
FIG. 44 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 1200 and the security module 1300 according to the fifth embodiment of the invention;
FIG. 45 shows a procedure in the descrambling process by means of the descrambling process unit 1207 in detail; and
FIG. 46 shows one example of the data structure of an I picture list descriptor.

DESCRIPTION OF THE PREFERRED EMBODIMENT

First Embodiment

<Summary>

[0097] A system for providing a storage service according to the first embodiment of the invention consists of a broadcast apparatus, a reception apparatus, and a security module.

[0098] The broadcast apparatus generates a scrambling key list including all of the scrambling keys necessary for descrambling scrambled content, includes the list in an ECM for storage (hereafter called "storage ECM"), and broadcasts the scrambled content accompanied with the ECM.

[0099] The security module, which is integrated with the reception apparatus in a predetermined position, receives and stores the storage ECM and the scrambled content, decodes the ECM for storage in return for the paid charges, and sequentially descrambles the received scrambled content using the scrambling key list included in the storage ECM.

<Overall Construction>

[0100] FIG. 1 shows the construction of the system for providing a storage service according to the first embodiment of the invention. The system shown in FIG. 1 consists of a broadcast apparatus 100, a reception apparatus 200, and a security module 300.

[0101] Note that, in FIG. 1, a scrambling key recording unit 10 which records scrambling keys and a content recording unit 11 which records content are shown for explanation.

[0102] The security module 300 is a portable and intelligent recording medium such as an IC card. The security module 300 is set in a predetermined position of the reception apparatus 200 and used together with the reception apparatus 200.

(Construction of Broadcast Apparatus)

[0103] The broadcast apparatus 100 shown in FIG. 1 consists of a TS packetizing unit 101, a scrambling key list generation unit 102, a scrambling process unit 103, an ECM generation unit 104, a multiplexing unit 105, a content acquisition unit 106, and a scrambling key acquisition unit 107.

[0104] The content acquisition unit 106 acquires content including visual, audio, and text data recorded in the content recording unit 11.

[0105] The TS packetizing unit 101 converts the content acquired by the content acquisition unit 106 into transport stream (hereafter abbreviated as "TS") packets.

[0106] Note that the TS packet has the fixed length of 188 bytes as prescribed by the MPEG-2 standard.

[0107] The scrambling key acquisition unit 107 acquires scrambling keys recorded in the scrambling key recording unit 10.

[0108] The scrambling key list generation unit 102 generates a scrambling key list base on the scrambling keys acquired by the scrambling key acquisition unit 107.

[0109] Note that the scrambling key list is represented

by scrambling key list descriptors, for example.

[0110] FIG. 2 shows one example of the data structure of a scrambling key list descriptor.

[0111] The scrambling key list descriptor shown in FIG. 2 includes a scrambling key identifier (Ks_id) for identifying a scrambling key, the scrambling key(Ks), and the number of TS packets to be scrambled with the scrambling key(TS_packet_number). In the list, the scrambling key identifiers(Ks_id), the scrambling keys (Ks), and the number of TS packets are described as much as the number of scrambling keys.

[0112] The scrambling process unit 103 scrambles the content converted into TS packets by the TS packetizing unit 101, based on the scrambling key list generated by the scrambling key list generation unit 102. The detailed description on the scrambling process unit 103 will be given later.

[0113] The ECM generation unit 104 generates ECMs for normal reproduction (hereafter called "normal reproduction ECM"), which are the same as in the conventional system, and also generates storage ECMs including the scrambling key list generated by the scrambling key list generation unit 102.

[0114] Note that the storage ECM is used for reproducing the stored scrambled content.

[0115] FIG. 3 shows one example of the data structure of a storage ECM.

[0116] The storage ECM shown in FIG.3 is generated by adding the scrambling key list descriptor as described above to a variable portion (a target to be encoded) in the main body of the ECM as prescribed by the ARIB (The Association of Radio Industries and Businesses) standard.

[0117] In a storage ECM, information for distinguishing the storage ECM from a normal reproduction ECM is also embedded. For instance, different values may be set at the table identifiers described in the section header for the storage ECM and the normal reproduction ECM. Alternatively, different values may be set at the extended table identifiers for the both ECMs, while the same value being set at the table identifiers for them.

[0118] The multiplexing unit 105 attaches/attaches the generated normal reproduction ECM with/to the scrambled content, multiplexes it with a storage ECM to produce a TS, and broadcasts the TS.

[0119] The following describes transmission timing for the storage ECM.

[0120] Since one scrambling key list has only to be transmitted for each piece of scrambled content, the storage ECM may be transmitted in a time period longer than the transmission period for the conventional ECM.

[0121] FIG. 4 shows transmission timing for the scrambling key list.

[0122] As shown in FIG. 4, in the BS digital broadcasting system, the storage ECM may be transmitted in the time period approximately ten times as long as for the conventional ECM. In the environment where ECMs can be securely stored without any reception errors and storage errors, one storage ECM has only to be transmitted while all of the scrambled content associated with the storage ECM have been transmitted once.

[0123] FIG. 5 shows the detailed construction of the scrambling process unit 103.

[0124] The scrambling process unit 103 shown in FIG. 5 consists of a TS packet counting unit 110, a scrambling key list holding unit 111, a scrambling unit 112, and a scrambling key list interpretation unit 113.

[0125] The TS packet counting unit 110 acquires the content converted into TS packets by the TS packetizing unit 101 one TS packet at a time and passes it to the scrambling unit 112. The TS packet counting unit 110 also counts the TS packet cumulative number indicating the ordinal position of the acquired TS packet counted from the beginning of the content, and passes the number to the scrambling key list interpretation unit 113. The TS packet counting unit 110 resets the TS packet cumulative number into zero when other content starts to be processed.

[0126] The scrambling key list holding unit 111 acquires the scrambling key list generated by the scrambling key list generation unit 102 and holds it therein.

[0127] The scrambling key list interpretation unit 113 extracts the scrambling key corresponding to the TS packet to be scrambled from the scrambling key list stored in the scrambling key list holding unit 111, based on the TS packet cumulative number passed from the TS packet counting unit 110, and passes the extracted key to the scrambling unit 112.

[0128] FIG. 6 shows a relation between content and scrambling keys in a TS.

[0129] As shown in FIG. 6, this TS consists of four hundreds of TS packets obtained by converting content to be scrambled. Scrambling keys are changed, every one hundred of TS packets.

[0130] FIG. 7 shows the scrambling key list associated with the TS shown in FIG. 6.

[0131] As shown in FIG. 7, in this scrambling key list, the scrambling key associated with the leading one hundreds of TS packets is Ks1, the scrambling key associated with the TS packets from the 101st to 200th is Ks2, the scrambling key associated with the TS packets from the 201st to 300th is Ks3, and the scrambling key associated with the TS packets from the 301st to the 400th is Ks 4.

[0132] The scrambling unit 112 scrambles one TS packet passed from the TS packet counting unit 110 using the scrambling key passed from the scrambling key list interpretation unit 113 and passes it to the multiplexing unit 105. The scrambling unit 112 repeats this process until all TS packets have been processed.

(Construction of Reception Apparatus and Security Module)

[0133] The reception apparatus 200 shown in FIG. 1 consists of a TS separation unit 201, an HDD 202, a

scrambling key list holding unit 203, a descrambling process unit 204, and a reproduction unit 205.

[0134] The security module 300 shown in FIG. 1 is made up of an ECM interpretation unit 301.

[0135] The TS separation unit 201 receives a TS broadcast from the multiplexing unit 105, distinguishes between a normal reproduction ECM and a storage ECM based on the value of the table identifier or the extended table identifier, and separates the storage ECM and scrambled content.

[0136] The HDD 202 is a recording medium such as a hard disk drive. The HDD 202 stores the storage ECM and the scrambled content separated by the TS separation unit 201.

[0137] The ECM interpretation unit 301 extracts a scrambling key list from the storage ECM stored in the HDD 202.

[0138] The scrambling key list holding unit 203 holds the scrambling key list extracted by the ECM interpretation unit 301.

[0139] The descrambling process unit 204 descrambles the scrambled content stored in the HDD 202 based on the scrambling key list held by the scrambling key list holding unit 203 and passes it to the reproduction unit 205. Detailed description on the descrambling process unit 204 will be given later.

[0140] The reproduction unit 205 reproduces the descrambled content.

[0141] FIG. 8 shows the detailed construction of the descrambling process unit 204.

[0142] The descrambling process unit 204 shown in FIG. 8 is made up of a TS packet extraction unit 210, a descrambling unit 211, and a scrambling key list interpretation unit 212.

[0143] The TS packet extraction unit 210 extracts the scrambled content stored in the HDD 202 one TS packet at a time to pass it to the descrambling unit 211. Also, the TS packet extraction unit 210 counts the TS packet index indicating shows the ordinal position of the extracted TS packet counted from the beginning of the content and passes the index to the scrambling key list interpretation unit 212. Here, the TS packet extraction unit 210 resets the TS packet index into zero when other content start to be processed.

[0144] The scrambling key list interpretation unit 212 extracts the scrambling key corresponding to the TS packet index passed from the TS packet extraction unit 210 from the scrambling key list held by the scrambling key list holding unit 203 and passes it to the descrambling unit 211.

[0145] The descrambling unit 211 descrambles one TS packet passed from the TS packet extraction unit 210 using the scrambling key extracted by the scrambling key list interpretation unit 212 and passes it to the reproduction unit 205. The descrambling unit 211 repeats this process until all TS packets have been processed.

<Operations>

(Operations of Broadcast Apparatus)

[0146] FIG. 9 shows a procedure in the broadcasting process by means of the broadcast apparatus 100 according to the first embodiment of the invention.

[0147] Following describes the outline of the procedure with reference to FIG. 9.

(1) The content acquisition unit 106 acquires content such as image, sounds, and text data recorded in the content recording unit 11 (Step S1).
(2) The TS packetizing unit 101 converts the content acquired by the content acquisition unit 106 into TS packets (Step S2).
(3) The scrambling key acquisition unit 107 acquires the scrambling key recorded in the scrambling key recording unit 10 (Step S3).
(4) The scrambling key list generation unit 102 generates a scrambling key list based on the scrambling key acquired by the scrambling key acquisition unit 107 (Step S4).
(5) The scrambling process unit 103 scrambles the content converted into TS packets by the TS packetizing unit 101, based on the scrambling key list generated by the scrambling key list generation unit 102 (Step S5).
(6) The ECM generation unit 104 generates a normal reproduction ECM and generates a storage ECM including the scrambling key list generated by the scrambling key list generation unit 102 (Step S6).
(7) The multiplexing unit 105 associates/attaches the generated normal reproduction ECM to/with to the scrambled content, multiplexes it with the storage ECM to generate TS, and broadcasts the TS (Step S7).

[0148] FIG. 10 shows a procedure in the scrambling process by means of the scrambling process unit 103 in detail.

[0149] Following describes the outline of the detailed procedure in the scrambling process, with reference to FIG. 10.

(1) The TS packet counting unit 110 resets the TS packet cumulative number into zero (Step S11).
(2) The TS packet counting unit 110 judges whether there are unprocessed TS packets or not (Step S12). If there are no any unprocessed TS packets, the scrambling process ends.
(3) If there are unprocessed TS packets, the TS packet counting unit 110 acquires one unprocessed TS packet to pass it to the scrambling unit 112, and counts the TS packet cumulative number to pass it to the scrambling key list interpretation unit 113 (Step S13).
(4) The scrambling key list interpretation unit 113

extracts the scrambling key corresponding to the TS packet now being processed from the scrambling key list stored in the scrambling key list holding unit 111, based on the TS packet cumulative number passed from the TS packet counting unit 110 (Step S14).
(5) The scrambling unit 112 scrambles one TS packet passed from the TS packet counting unit 110 using the scrambling key passed from the scrambling key list interpretation unit 113 and passes it to the multiplexing unit 105. Then, the procedure returns upward to process the successive TS packet(Step S15).

(Operations of Reception Apparatus)

[0150] FIG. 11 shows a procedure in the reception and storage processes by means of the reception apparatus 200 and the security module 300 according to the first embodiment of the invention.
[0151] Following describes the outline of the processes with reference to FIG. 11.

(1) The TS separation unit 201 receives a TS broadcast from the multiplexing unit 105. Then, the TS separation unit 201 distinguishes a normal reproduction ECM and a storage ECM based on the value of the table identifier or the extended table identifier, and separates the storage ECM and scrambled content (Step S21).
(2) The HDD 202 stores the storage ECM and the scrambled content separated by the TS separation unit 201 (Step S22).

[0152] Note that, the storage ECM and the scrambled content may be separated not at this stage but later (e.g., before using them).
[0153] FIG. 12 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 200 and the security module 300 according to the first embodiment of the invention.
[0154] Following describes the outline of the procedure in the reproduction process, with reference to FIG. 12.

(1) The ECM interpretation unit 301 extracts the scrambling key list from the storage ECM stored in the HDD 202 (Step S31).
(2) The scrambling key list holding unit 203 holds the scrambling key list extracted by the ECM interpretation unit 301 (Step S32).
(3) The descrambling process unit 204 descrambles the scrambled content stored in the HDD 202 based on the scrambling key list held by the scrambling key list holding unit 203 and passes it to the reproduction unit 205 (Step S33).
(4) The reproduction unit 205 reproduces the descrambled content (Step S34).

[0155] FIG. 13 shows a procedure in the descrambling process by means of the descrambling process unit 204 in detail.
[0156] Following describes the outline of the detailed procedure in the descrambling process, with reference to FIG. 13.

(1) The TS packet extraction unit 210 resets the TS packet index into zero when other content starts to be processed (Step S41).
(2) The TS packet extraction unit 210 judges whether there are unprocessed TS packets or not (Step S42). If there are not any unprocessed TS packet, the descrambling process ends.
(3) If there are unprocessed TS packets, the TS packet extraction unit 210 extracts one unprocessed TS packet to pass it to the descrambling unit 211. Also, the TS packet extraction unit 210 counts the TS packet index to pass it to the scrambling key list interpretation unit 212 (Step S43).
(4) The scrambling key list interpretation unit 212 extracts the scrambling key corresponding to the TS packet index passed from the TS packet extraction unit 210, from the scrambling key list held by the scrambling key list holding unit 203, and passes it to the descrambling unit 211 (Step S44).
(5) The descrambling unit 211 descrambles one TS packet passed from the TS packet extraction unit 210 using the scrambling key extracted by the scrambling key list interpretation unit 212 and passes it to the reproduction unit 205. Then, the procedure returns upward to process the successive TS packet (Step S45).

[0157] Following describes the procedure of the particular reproduction process after the above-described reception and storage processes.
[0158] FIG. 14 is a schematic view showing an image stream in the MPEG-2 coding system.
[0159] As shown in FIG. 14, according to the MPEG-2 coding system, the image stream consists of three kinds of pictures: I pictures (intraframe-coded picture), B pictures (bidirectional frame), and P pictures (predictive picture). Among these pictures, only I picture can be drawn and displayed based solely on the data that it contains.
[0160] Therefore, the fast forward reproduction mode, which is one of typical particular reproduction processes, can be realized by selecting only I pictures to reproduce content.
[0161] FIG. 15 shows a TS obtained by converting the image stream shown in FIG. 14.
[0162] In FIG. 15, the diagonally shaded portions are the TS packets obtained by converting the I pictures shown in FIG. 14. Pictures I1, I2, I3, and I4 are converted into TSP1 to TSP4, TSP101 to TSP104, TSP201 to TSP204, and TSP301 to TSP304, respectively.

[0163] The procedure of the fast forward reproduction, which is one of typical particular reproduction processes, is almost the same as that of the reproduction process shown in FIG. 12. However, the detailed procedure in the descrambling process by means of the descrambling process unit 204 is different from that shown in FIG. 12.

[0164] FIG. 16 shows a procedure in the descrambling process in the fast-forward reproduction mode in detail. Note that the same numerals are assigned to the step in which the same processes as in FIG. 13 are conducted, and explanation for them has been omitted.

[0165] Following describes the outline of the detailed procedure in the descrambling process in the fast forward reproduction mode, with reference to FIGS. 7 and 13 to 16.

(1) Same as the step (1) in FIG. 13 (Step S41)
(2) Same as the step (2) in FIG. 13 (Step S42)
(3) Same as the step (3) in FIG. 13 (Step S43)
For instance, when extracting TSP1 shown in FIG. 15, the TS packet extraction unit 210 counts the TS packet index as one, because TSP1 is the first packet.
(4) The descrambling process unit 204 judges whether the process is the fast forward reproduction process or not (Step S51). If the process is not the fast forward reproduction process, the procedure goes to the process for extracting a scrambling key (to Step S44).
(5) If the process is the fast forward reproduction process, the descrambling process unit 204 judges whether the extracted TS packet is the TS packet obtained by converting an I picture or not (Step S52). If the packet is not the TS packet obtained by converting an I picture, the procedure returns upward to process the successive TS packet.
Note that, as one method for judging whether the extracted TS packet is the TS packet obtained by converting an I picture or not, the broadcast apparatus may embed the information indicative of I picture in the unscrambled portion in the TS packet, and the reception apparatus may make a judgement based on the information. The Japanese Laid-Open Patent Application No. 8-340541 discloses such a method.
When extracting the TSP1 shown in FIG. 15, the descrambling process unit 204 judges the TSP1 as the TS packet obtained by converting an I picture.
(6) Same as the step (4) in FIG. 13 (Step S44)
For instance, the scrambling key list interpretation unit 212 extracts the scrambling key Ks1 corresponding to the TS packet index 1 from the scrambling key list shown in FIG. 7.
(7) Same as the step (5) in FIG. 13 (Step S45)

[0166] For instance, the descrambling unit 211 descrambles TSP2 shown in FIG.15 using the scrambling key Ks1.

[0167] Similarly, TSP1 to TSP4, TSP101 to TSP104, TSP201 to TSP204, and TSP301 to TSP304 are descrambled with the scrambling keys Ks1, Ks2, Ks3, and Ks 4, respectively.

[0168] Note that, The reverse reproduction process can be realized by reversing the extraction order of TS packets in the normal reproduction process.

[0169] In addition, the fast reverse reproduction process can be realized by reversing the extraction order of TS packets in the fast forward reproduction process.

[0170] Moreover, the random access reproduction process can be realized by altering the starting position of the TS packet to be extracted.

[0171] As stated above, according to the first embodiment, various particular reproduction processes can be realized by extracting a scrambling key corresponding to any one of TS packets from the scrambling key list using the TS packet index.

Embodiment 2

<Summary>

[0172] The broadcast apparatus according to the second embodiment of the invention has the same construction as in the above first embodiment, but the reception apparatus and the security module have different constructions.

[0173] The first embodiment is predicted on that information does not leak out of the reception apparatus so as to provide adequate security of information, and therefore the scrambling key list is held in the reception apparatus. Whereas, according to the second embodiment, the scrambling key list is held in the security module and not in the reception apparatus, whereby the security against the leakage of the scrambling key list can be improved.

<Overall Construction>

[0174] FIG. 17 shows a portion of the construction of a system for providing a storage service according to the second embodiment of the invention.

[0175] The system shown in FIG. 17 is made up of a broadcast apparatus 100, a reception apparatus 400, and a security module 500. Note that the broadcast apparatus is not illustrated in FIG. 17, because the apparatus is the same as in the first embodiment.

[0176] The security module 500 is a portable and intelligent recording medium such as an IC card. The security module 500 is set in a predetermined position of the reception apparatus 400 and used together with the reception apparatus 400.

[0177] Note that construction elements which have the same functions as those in the first embodiment have been given the same reference numerals and their explanation has been omitted.

(Construction of Broadcast Apparatus)

[0178] The construction of the broadcast apparatus has been omitted, because it is the same as in the first embodiment.

(Constructions of Reception Apparatus and Security Module)

[0179] The reception apparatus shown in FIG. 17 is made up of a TS separation unit 201, an HDD 202, a descrambling process unit 401, and a reproduction unit 205.

[0180] The security module shown in FIG. 17 is made up of an ECM interpretation unit 301, a scrambling key list holding unit 501, and a scrambling key list interpretation unit 502.

[0181] The scrambling key list holding unit 501 holds the scrambling key list extracted by the ECM interpretation unit 301.

[0182] The descrambling process unit 401 extracts the scrambled content stored in the HDD 202 one TS packet at a time and counts the TS packet index to pass them to the scrambling key list interpretation unit 502. Then, on receiving the scrambling key corresponding to the TS packet index from the scrambling key list interpretation unit 502, the descrambling process unit 401 descrambles the TS packet using the scrambling key and passes it to the reproduction unit 205. Detailed description on the descrambling process unit 401 will be given later.

[0183] The scrambling key list interpretation unit 502 extracts the scrambling key corresponding to the TS packet index passed from the descrambling process unit 401, from the scrambling key list held by the scrambling key list holding unit 501, and passes the extracted key to the descrambling process unit 401.

[0184] FIG. 18 shows the detailed construction of the descrambling process unit 401.

[0185] The descrambling process unit 401 shown in FIG. 18 is made up of the TS packet extraction unit 410 and the descrambling unit 411.

[0186] The TS packet extraction unit 410 extracts the scrambled content stored in the HDD 202 one TS packet at a time to pass it to the descrambling unit 411. Also, the TS packet extraction unit 410 counts the TS packet index indicating the ordinal position of the extracted TS packet counted from the beginning of the content and passes it to the scrambling key list interpretation unit 502. Here, the TS packet extraction unit 410 resets the TS packet index into zero when other content start to be processed.

[0187] The descrambling unit 411 descrambles one TS packet passed from the TS packet extraction unit 410 with the scrambling key passed from the scrambling key list interpretation unit and passes it to the reproduction unit 205. The descrambling unit 411 repeats this process until all TS packets have been processed.

(Operations)

[0188] Since operations in this embodiment are the same as in the first embodiment, their explanation has been omitted.

[0189] As described above, according to the second embodiment of the invention, various particular reproduction processes can be realized, while improving the security against the leakage of the scrambling key list by extracting a scrambling key corresponding to any one of TS packets from the scrambling key list held in the security module.

Embodiment 3

<Summary>

[0190] According to the third embodiment of the invention, correspondences between TS packets and scrambling keys are described in the ECM, and the value of Continuity Counter (CC) described in the unscrambled portion in the TS packet is utilized, whereby the number of TS packets to be scrambled (TS_packet_number) does not need to be described in the scrambling key list descriptor, which leads to decrease in the amount of data to be transmitted.

<Overall Construction>

[0191] FIG. 19 shows a portion of the construction of a system for providing a storage service according to the third embodiment of the invention.

[0192] The system shown in FIG. 19 is made up of a broadcast apparatus 600, a reception apparatus 700, and a security module 300.

[0193] Note that construction elements which have the same functions as those in the first embodiment have been given the same reference numerals and their explanation has been omitted.

(Construction of Broadcast Apparatus)

[0194] The broadcast apparatus shown in FIG. 19 is made up of a TS packetizing unit 101, a scrambling key list generation unit 102, a scrambling process unit 601, an ECM generation unit 104, a multiplexing unit 105, a content acquisition unit 106, and a scrambling key list acquisition unit 107.

[0195] The scrambling process unit 601 scrambles the content converted into TS packets by the TS packetizing unit 101 based on the scrambling key list generated by the scrambling key list generation unit 102.

[0196] FIG. 20 shows the detailed construction of the scrambling process unit 601.

[0197] The scrambling process unit 601 shown in FIG. 20 is made up of a scrambling key identifier calculation unit 610, a TS packet header interpretation unit 611, a scrambling key list holding unit 612, a scrambling unit

613, and a scrambling key list interpretation unit 614.

[0198] The TS packet header interpretation unit 611 acquires the content converted into TS packets by the TS packetizing unit 101 one TS packet at a time to pass it to the scrambling unit 613. Also, the TS packet header interpretation unit 611 reads the value of Continuity Counter (CC) to pass it to the scrambling key identifier calculation unit 610.

[0199] Note that the CC is a cyclic counter using the four-bit value of the header in the TS packet as prescribed by the MPEG-2 coding system as the international standard. The CC increments one by one from zero to fifteen, and then returns to zero, which is used to determine if any TS packets with the same packet ID are abandoned partway.

[0200] The scrambling key identifier calculation unit 610 calculates a scrambling key identifier using the value of the CC passed from the TS packet header interpretation unit 611 and passes it to the scrambling key list interpretation unit 614.

[0201] One method for calculating a scrambling key identifier from the value of the CC is that the value of "CC mod n" (where $1 \leqq n \leqq 16$) is set at the scrambling key identifier. Here, "A mod B" indicates the remainder obtained by dividing A by B.

[0202] For instance, in the case of n=16, there are sixteen kinds of scrambling key identifiers (i.e., 0 to 15). As for the TS packet whose value is 2, for example, the scrambling key identifier is 2, because the remainder obtained by dividing 2 by 16 is 2.

[0203] The scrambling key list holding unit 612 acquires and holds the scrambling key list generated by the scrambling key list generation unit 102.

[0204] FIG. 21 shows the scrambling key list in the case that the value of "CC mod 16" is set at the scrambling key identifier.

[0205] The scrambling key list interpretation unit 614 extracts the scrambling key corresponding to the TS packet to be scrambled from the scrambling key list stored in the scrambling key list holding unit 612, based on the scrambling key identifier passed from the scrambling key identifier calculation unit 610 and passes it to the scrambling unit 613.

[0206] For instance, in the case that the scrambling key identifier is 2, the scrambling key Ks3 is extracted according to the scrambling key list shown in FIG. 21.

[0207] The scrambling unit 613 scrambles one TS packet passed from the TS packet header interpretation unit 611 using the scrambling key passed from the scrambling key list interpretation unit 614 and passes it to the multiplexing unit 105. The scrambling unit 613 repeats this process until all TS packets have been processed.

[0208] For instance, in the case that the scrambling key Ks3 is extracted, scrambling process is conducted with the scrambling key Ks3.

[0209] That is the explanation for the case of n=16. Naturally, n is not limited to 16.

[0210] That is, n may be any number between 1 and 15. After generating a scrambling key list by changing the value of n, the number of used scrambling keys can be easily altered without generating the list again. For instance, by changing the value of n to 4 without changing the scrambling key list shown in FIG. 21, the value of identifier can be any number between 0 and 3. As a result, the four types of scrambling keys (Ks1, Ks2, Ks3, and Ks4)can be used. Note that the value of n may be stored as a calculation method or a fixed value in advance, and the method and the value may be described in the variable portion in the storage ECM shown in FIG. 3.

[0211] Alternatively, instead of calculating a scrambling key identifier from the value of CC, the scrambling key identifier may be calculated from the specific bits of the Program Clock Reference (PCR) or the Original PCR (OPCR), which are also prescribed by the MPEG-2 coding system as the international standard.

[0212] For example, using the specific four-bit values in the PCR or OPCR, the scrambling key identifier may be calculated in the same manner as in the above process using the value of CC.

[0213] Otherwise, instead of using the value prescribed by the MPEG-2 coding system, users may directly describe the value of the scrambling key identifier in the area where the application is not specified but which users can utilize freely, such as private data area in the Adaptation Field.

(Constructions of Reception Apparatus and Security Module)

[0214] The reception apparatus shown in FIG. 19 is made up of a TS separation unit 201, an HDD 202, a scrambling key list holding unit 203, a descrambling process unit 701, and a reproduction unit 205.

[0215] The descrambling process unit 701 descrambles the scrambled content stored in the HDD 202, based on the scrambling key list held by the scrambling key list holding unit 203 and passes it to the reproduction unit 205.

[0216] FIG. 22 shows the detailed construction of the descrambling process unit 701.

[0217] The descrambling process unit 701 shown in FIG. 22 is made up of a TS packet extraction unit 710, a scrambling key identifier calculation unit 711, a descrambling unit 712, and a scrambling key list interpretation unit 713.

[0218] The TS packet extraction unit 710 extracts the scrambled content stored in the HDD 202 one TS packet at a time to pass it to the descrambling unit 712. Also, the TS packet extraction unit 710 reads the value of the CC in the extracted TS packet to pass it to the scrambling key identifier calculation unit 711.

[0219] The scrambling key identifier calculation unit 711 calculates a scrambling key identifier from the value of the CC passed from the TS packet extraction unit 710 and passes it to the scrambling key list interpretation unit

713.

[0220] The scrambling key list interpretation unit 713 extracts the scrambling key corresponding to the TS packet to be scrambled from the scrambling key list stored in the scrambling key list holding unit 203, based on the scrambling key identifier passed from the scrambling key identifier calculation unit 711, and passes it to the descrambling unit 712.

[0221] The descrambling unit 712 descrambles one TS packet passed from the TS packet extraction unit 710 using the scrambling key passed from the scrambling key list interpretation unit 713 and passes it to the reproduction unit 205. The descrambling unit 712 repeats this process until all TS packets have been processed.

<Operations>

(Operations of Broadcast Apparatus)

[0222] FIG. 23 shows a procedure in the broadcasting process by means of the broadcast apparatus 600 according to the third embodiment of the invention. Note that the same numerals are assigned to the step where the same processes as in FIG. 9 are conducted, and explanation for them has been omitted.

[0223] Following describes the outline of the procedure in the broadcasting process, with reference to FIG. 23.

(1) Same as the step (1) in FIG. 9 (Step S1)
(2) Same as the step (2) in FIG.9 (Step S2)
(3) Same as the step (3) in FIG.9 (Step S3)
(4) Same as the step (4) in FIG.9 (Step S4)
(5) The scrambling process unit 601 scrambles the content converted into TS packets by the TS packetizing unit 101, based on the scrambling key list generated by the scrambling key list generation unit 102 (Step S51).
(6) Same as the step (6) in FIG.9 (Step S6)
(7) Same as the step (7) in FIG. 9 (Step S7)

[0224] FIG. 24 shows a procedure in the scrambling process by means of the scrambling process unit 601 in detail.

[0225] Following describes the outline of the detailed procedure in the scrambling process, with reference to FIG. 24.

(1) The TS packet header interpretation unit 611 judges whether there are any unprocessed TS packets or not (Step S61). If there are not any unprocessed TS packets, the scrambling process ends.
(2) If there are unprocessed TS packets, the TS packet header interpretation unit 611 acquires one unprocessed TS packet to pass it to the scrambling unit 613, and reads the value of the CC to pass it to the scrambling key identifier calculation unit 610 (Step S62).
(3) The scrambling key identifier calculation unit 610 calculates a scrambling key identifier from the value of the CC passed from the TS packet header interpretation unit 611 to pass it to the scrambling key list interpretation unit 614 (Step S63).
(4) The scrambling key list interpretation unit 614 extracts the scrambling key corresponding to the TS packet now being processed, from the scrambling key list stored in the scrambling key list holding unit 612, based on the scrambling key identifier passed from the scrambling key identifier calculation unit 610 and passes the extracted key to the scrambling unit 613 (Step S64).
(5) The scrambling unit 613 scrambles one TS packet passed from the TS packet header interpretation unit 611 using the scrambling key passed from the scrambling key list interpretation unit 614 and passes it to the multiplexing unit 105. Then, the procedure returns upward to process the successive TS packet (Step S65)

(Operations of Reception Apparatus)

[0226] Explanation of the procedure in the reception and storage processes by means of the reception apparatus 700 and the security module 300 according to the third embodiment of the invention has been omitted, because they are the same as in the first embodiment.

[0227] FIG. 25 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 700 and the security module 300 according to the third embodiment of the invention. Note that the same numerals are assigned to the step where the same processes as in FIG. 12 are conducted, and explanation for them has been omitted.

[0228] Following describes the outline of the procedure in the reproduction process, with reference to FIG. 25.

(1) Same as the step (1) in FIG. 12 (Step S31)
(2) Same as the step (2) in FIG. 12 (Step S32)
(3) The descrambling process unit 701 descrambles the scrambled content stored in the HDD 202 based on the scrambling key list held by the scrambling key list holding unit 203 and passes the descrambled content to the reproduction unit 205 (Step S71).
(4) Same as the step (4) in FIG. 12 (Step S34)

[0229] FIG. 26 shows a procedure in the descrambling process by means of the descrambling process unit 701 in detail.

[0230] Following describes the outline of the detailed procedure in the descrambling process, with reference to FIG. 26.

(1) The TS packet extraction unit 710 judges whether there are any unprocessed TS packets or not (Step S81). If there are no any unprocessed TS packets,

the descrambling process ends.

(2) If there are unprocessed TS packets, the TS packet extraction unit 710 extracts one unprocessed TS packet to pass it to the scrambling unit 712, and reads the value of the CC of the extracted TS packet to pass it to the scrambling key identifier calculation unit 711 (Step S82).

(3) The scrambling key identifier calculation unit 711 calculates a scrambling key identifier from the value of the CC passed from the TS packet extraction unit 710 and passes it to the scrambling key list interpretation unit 713 (Step S83).

(4) The scrambling key list interpretation unit 713 extracts the scrambling key from the scrambling key list stored in the scrambling key list holding unit 203, based on the scrambling key identifier passed from the scrambling key identifier calculation unit 711 and passes the extracted key to the descrambling unit 712 (Step S84).

(5) The descrambling unit 712 descrambles one TS packet passed from the TS packet extraction unit 710 using the scrambling key passed from the scrambling key list interpretation unit 713 and passes the descrambled TS packet to the reproduction unit 205. Then, the procedure returns upward to process the successive TS packet(Step S85).

[0231] As stated above, according to the third embodiment of the invention, various particular reproduction processes can be realized by extracting a scrambling key corresponding to any one of TS packets from the scrambling key list using the value of CC.

[0232] Note that, instead of the value of CC, any one of the number of TS packets, the cumulative amount of data, a relative reproduction time, and an identifier for a scrambling key may be used.

Embodiment 4

<Summary>

[0233] A system for providing a storage service according to the fourth embodiment of the invention consists of a broadcast apparatus, a reception apparatus, and a security module.

[0234] Unlike the first embodiment, the broadcast apparatus according to the fourth embodiment does not generate the scrambling key list. Instead, the broadcast apparatus in this embodiment adds auxiliary information including identifying information on the scrambled content such as packet numbers so as to help the reception apparatus to generate a scrambling key list, the scrambling keys, and the like, to the normal reproduction ECM to broadcast it together with the scrambled content.

[0235] The security module, which is set and integrated with the reception apparatus in a predetermined position, receives the normal reproduction ECM and the scrambled content, stores the scrambled content while generating a scrambling key list based on the auxiliary information added to the normal reproduction ECM, and sequentially descrambles the scrambled content using the stored scrambling key list.

<Overall Construction>

[0236] FIG. 27 shows the construction of a system for providing a storage service according to the fourth embodiment of the invention.

[0237] The system shown in FIG. 27 is made up of a broadcast apparatus 800, a reception apparatus 900, and a security module 1000.

[0238] The security module 1000 is a portable and intelligent recording medium such as an IC card. The security module 1000 is set in a predetermined position of the reception apparatus 900 and used together with the reception apparatus 900.

[0239] Note that construction elements which have the same functions as those in the first embodiment have been given the same reference numerals and the same names and their explanation has been omitted.

(Construction of Broadcast Apparatus)

[0240] The broadcast apparatus 800 shown in FIG. 27 is made up of a TS packetizing unit 101, an auxiliary information generation unit 801, a scrambling process unit 802, an ECM generation unit 803, a multiplexing unit 804, a content acquisition unit 106, and a scrambling key acquisition unit 107.

[0241] The auxiliary information generation unit 801 generates auxiliary information based on the scrambling key acquired by the scrambling key acquisition unit 107.

[0242] Note that the auxiliary information is represented by scrambling key list generation descriptors, for example.

[0243] FIG. 28 shows one example of the data structure of the scrambling key list generation descriptor.

[0244] The scrambling key list descriptor shown in FIG. 28 includes a scrambling key identifier (Ks_id) for identifying a scrambling key, the scrambling key(Ks), and the number of TS packets to be scrambled with the scrambling key (TS_packet_number).

[0245] The scrambling process unit 802 scrambles the content converted into TS packets by the TS packetizing unit 101, based on the auxiliary information generated by the auxiliary information generation unit 801. The detailed description on the scrambling process unit 802 will be given later.

[0246] The ECM generation unit 803 generates a normal reproduction ECM, and adds the auxiliary information generated by the auxiliary information generation unit 801 to the normal reproduction ECM.

[0247] FIG. 29 shows one example of the data structure of a normal reproduction ECM, to which the scrambling key list generation descriptor is added.

[0248] The normal reproduction ECM shown in FIG.

29 is generated by adding the scrambling key list generation descriptor as described above to a variable portion (a target to be encoded) in the main body of the ECM as prescribed by the ARIB (The Association of Radio Industries and Businesses) standard.

[0249] The multiplexing unit 804 associates/attaches the scrambled content with/to the generated normal reproduction ECM to produce a TS, and broadcasts the TS.

[0250] FIG. 30 shows the detailed construction of the scrambling process unit 802.

[0251] The scrambling process unit 802 shown in FIG. 30 is made up of a TS packet counting unit 810, an auxiliary information holding unit 811, a scrambling unit 812, and an auxiliary information interpretation unit 813.

[0252] The TS packet counting unit 810 acquires the content converted into TS packets by the TS packetizing unit 101 one TS packet at a time and passes it to the scrambling unit 812. The TS packet counting unit 110 also counts the TS packet cumulative number showing the ordinal position of the acquired TS packet counted from the beginning of the content, and passes the number to the auxiliary information interpretation unit 813. The TS packet counting unit 810 resets the TS packet cumulative number into zero when other content starts to be processed.

[0253] The auxiliary information holding unit 811 acquires and holds the auxiliary information generated by the auxiliary information generation unit 801.

[0254] The auxiliary information interpretation unit 813 extracts the scrambling key corresponding to the TS packet to be scrambled from the auxiliary information stored in the auxiliary information holding unit 811, based on the TS packet cumulative number passed from the TS packet counting unit 810, and passes the extracted key to the scrambling unit 812.

[0255] The scrambling unit 812 scrambles one TS packet passed from the TS packet counting unit 810 using the scrambling key passed from the auxiliary information interpretation unit 813 and passes the scrambled TS packet to the multiplexing unit 804. The scrambling unit 812 repeats this process until all TS packets have been processed.

(Constructions of Reception Apparatus and Security Module)

[0256] The reception apparatus 900 shown in FIG. 27 is made up of a TS separation unit 901, an HDD 902, a scrambling key list generation unit 903, a scrambling key list holding unit 904, a descrambling process unit 905, and a reproduction unit 205.

[0257] The security module 1000 shown in FIG. 27 is made up of an ECM interpretation unit 1001.

[0258] The TS separation unit 901 receives the TS broadcast by the multiplexing unit 804, and separates a normal reproduction ECM and scrambled content.

[0259] The HDD 902 is a recording medium such as a hard disk drive. The HDD 902 stores the normal reproduction ECM and the scrambled content separated by the TS separation unit 901.

[0260] The ECM interpretation unit 1001 extracts auxiliary information from the stored normal reproduction ECM.

[0261] The scrambling key list generation unit 903 generates a scrambling key list based on the auxiliary information extracted by the ECM interpretation unit 1001.

[0262] The scrambling key list holding unit 904 holds the scrambling key list generated by the scrambling key list generation unit 903.

[0263] The descrambling process unit 905 descrambles the scrambled content stored in the HDD 202 based on the scrambling key list held by the scrambling key list holding unit 904, and passes the descrambled content to the reproduction unit 205.

[0264] FIG. 31 shows the detailed construction of the descrambling process unit 905.

[0265] The descrambling unit 905 shown in FIG. 31 is made up of a TS packet extraction unit 910, a descrambling unit 911, and a scrambling key list interpretation unit 912.

[0266] The TS packet extraction unit 910 extracts the scrambled content stored in the HDD 902 one TS packet at a time and passes it to the descrambling unit 911. The TS packet extraction unit 910 also counts the TS packet index showing the ordinal position of the acquired TS packet counted from the beginning of the content, and passes the number to the scrambling key list interpretation unit 912. The TS packet extraction unit 910 resets the TS packet index into zero when other content starts to be processed.

[0267] The scrambling key list interpretation unit 912 extracts the scrambling key corresponding to the TS packet index passed from the TS packet extraction unit 910 from the scrambling key list held by the scrambling key list holding unit 904, and passes the extracted key to the descrambling unit 911.

[0268] The descrambling unit 911 descrambles one TS packet passed from the TS packet extraction unit 910 using the scrambling key extracted by the scrambling key list interpretation unit 912 and passes the descrambled TS packet to the reproduction unit 205. The descrambling unit 911 repeats this process until all TS packets have been processed.

<Operations>

(Operations of Broadcast Apparatus)

[0269] FIG. 32 shows a procedure in the broadcasting process by means of the broadcast apparatus 800 according to the fourth embodiment of the invention.

[0270] Following describes the outline of the procedure in the broadcast process, with reference to FIG. 32.

(1) Same as the step (1) in FIG. 9 (Step S1)
(2) Same as the step (2) in FIG. 9 (Step S2)

(3) Same as the step (3) in FIG. 9 (Step S3)
(4) The auxiliary information generation unit 801 generates auxiliary information based on the scrambling key acquired by the scrambling key acquisition unit 107 (Step S91).
(5) The scrambling process unit 802 scrambles the content converted into TS packets by the TS packetizing unit 101, based on the auxiliary information generated by the auxiliary information generation unit 801 (Step S92).
(6) The ECM generation unit 803 generates a normal reproduction ECM and adds the auxiliary information generated by the auxiliary information generation unit 801 to the normal reproduction ECM (Step S93).
(7) The multiplexing unit 804 associates/attaches the generated normal reproduction ECM with/to the scrambled content to produce TS and broadcasts the TS (Step S94).

[0271] FIG. 33 shows a procedure in the scrambling process by means of the scrambling process unit 802 in detail.

[0272] Following describes the outline of the detailed procedure in the scrambling process, with reference to FIG. 33.

(1) The TS packet counting unit 810 resets the TS packet cumulative number into zero (Step S101).
(2) The TS packet counting unit 810 judges whether there are any unprocessed TS packets or not (Step S102). If there are no any unprocessed TS packets, the scrambling process ends.
(3) If there are unprocessed TS packets, the TS packet counting unit 810 acquires one unprocessed TS packet to pass it to the scrambling unit 812, and counts the TS packet cumulative number to pass it to the auxiliary information interpretation unit 813 (Step S103).
(4) The auxiliary information interpretation unit 813 extracts the scrambling key corresponding to the TS packet now being processed from the auxiliary information stored in the auxiliary information holding unit 811, based on the TS packet cumulative number passed from the TS packet counting unit 810 (Step S104).
(5) The scrambling unit 812 scrambles one TS packet passed from the TS packet counting unit 810 using the scrambling key passed from the auxiliary information interpretation unit 813 and passes it to the multiplexing unit 804. Then, the procedure returns upward to process the successive TS packet(Step S105).

(Operations of Reception Apparatus)

[0273] FIG. 34 shows a procedure in the reception and storage processes by means of the reception apparatus 900 and the security module 1000 according to the fourth embodiment of the invention.

[0274] Following describes the outline of the processes with reference to FIG. 34.

(1) The TS separation unit 901 receives a TS broadcast by the multiplexing unit 804. Then, the TS separation unit 901 separates a normal reproduction ECM and scrambled content (Step S111).
(2) The HDD 202 stores the normal reproduction ECM and the scrambled content separated by the TS separation unit 901 (Step S112).
(3) The ECM interpretation unit 1001 extracts the auxiliary information from the normal reproduction ECM (Step S113).
(4) The scrambling key list generation unit 903 generates a scrambling key list, based on the auxiliary information extracted by the ECM interpretation unit 1001 (Step S114).
(5) The scrambling key list holding unit 904 holds the scrambling key list generated by the scrambling key list generation unit 903 (Step S115).

[0275] Note that, the normal reproduction ECM and the scrambled content may be separated not at this stage but later (e.g., before using them).

[0276] FIG. 35 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 900 and the security module 1000 according to the fourth embodiment of the invention. Note that the same numerals are assigned to the step where the same processes as in FIG. 12 are conducted, and explanation for them has been omitted.

[0277] Following describes the outline of the reproduction process, with reference to FIG. 35.

(1) The descrambling process unit 905 descrambles the scrambled content stored in the HDD 902 based on the scrambling key list held by the scrambling key list holding unit 904 and passes the descrambled content to the reproduction unit 205 (Step S121).
(2) Same as the step (4) in FIG. 12 (Step S34)

[0278] FIG. 36 shows a procedure in the descrambling process by means of the descrambling process unit 905 in detail.

[0279] Following describes the outline of the detailed procedure in the descrambling process, with reference to FIG. 36.

(1) The TS packet extraction unit 910 resets the TS packet index into zero when other content starts to be processed (Step S131).
(2) The TS packet extraction unit 910 judges whether there are unprocessed TS packets or not (Step S132). If there are not any unprocessed TS packet, the descrambling process ends.
(3) If there are unprocessed TS packets, the TS packet extraction unit 910 extracts one unprocessed

TS packet to pass it to the descrambling unit 911. Also, the TS packet extraction unit 910 counts the TS packet index to pass it to the scrambling key list interpretation unit 912 (Step S133).
(4) The scrambling key list interpretation unit 912 extracts the scrambling key corresponding to the TS packet index passed from the TS packet extraction unit 910, from the scrambling key list held by the scrambling key list holding unit 904, and passes the extracted key to the descrambling unit 911 (Step S134).
(5) The descrambling unit 911 descrambles one TS packet passed from the TS packet extraction unit 910 using the scrambling key extracted by the scrambling key list interpretation unit 912 and passes the descrambled TS packet to the reproduction unit 205. Then, the procedure returns upward to process the successive TS packet (Step S135).

[0280] In the fourth embodiment, in the case that a user has not made a contract to receive the content before receiving the content, the generated scrambling key list may be encoded and recorded, and then after making the contract the list may be decoded so as to be used. Alternatively, instead of generating the scrambling key list, all normal reproduction ECMs including auxiliary information may be stored when receiving the content, and then, after making the contract, the ECM interpretation unit 1001 may extract each piece of auxiliary information from all normal reproduction ECMs to generate the scrambling key list.
[0281] As described above, according to the fourth embodiment of the invention, various particular reproduction processes can be realized by extracting a scrambling key corresponding to any one of TS packets from the scrambling key list generated based on the auxiliary information when/after storing the scrambled content or the like.
[0282] Note here that the auxiliary information may be added to a storage ECM.

Embodiment 5

<Summary>

[0283] A system for providing a storage service according to the fifth embodiment of the invention consists of a broadcast apparatus, a reception apparatus, and a security module.
[0284] Unlike the first embodiment, the broadcast apparatus according to the fifth embodiment does not generate the scrambling key list. The broadcast apparatus in this embodiment broadcasts scrambled content together with normal reproduction ECMs.
[0285] The security module, which is set and integrated with the reception apparatus in a predetermined position, receives the normal reproduction ECM and the scrambled content, stores the scrambled content while generating a scrambling key list based on the normal reproduction ECM, and sequentially descrambles the scrambled content using the stored scrambling key list.

<Overall Construction>

[0286] FIG. 37 shows the construction of a system for providing a storage service according to the fifth embodiment of the invention.
[0287] The system shown in FIG. 37 is made up of a broadcast apparatus 1100, a reception apparatus 1200, and a security module 1300.
[0288] The security module 1300 is a portable and intelligent recording medium such as an IC card. The security module 1300 is set in a predetermined position of the reception apparatus 1200 and used together with the reception apparatus 1200.
[0289] Note that construction elements which have the same functions as those in the first embodiment have been given the same reference numerals and their explanation has been omitted.

(Construction of Broadcast Apparatus)

[0290] The broadcast apparatus 1100 shown in FIG. 37 is made up of a TS packetizing unit 101, a scrambling process unit 1101, an ECM generation unit 1102, a multiplexing unit 1103, a content acquisition unit 106, and a scrambling key acquisition unit 107.
[0291] The scrambling process unit 1101 scrambles the content converted into TS packets by the TS packetizing unit 101, based on the scrambling key acquired by the scrambling key acquisition unit 107. Note that explanation of the scrambling process by the scrambling process unit 1101 has been omitted, because the scrambling process is conducted in the same manner as in the current BS digital broadcasting system.
[0292] The ECM generation unit 1102 generates normal reproduction ECMs including scrambling keys acquired by the scrambling key acquisition unit 107.
[0293] The multiplexing unit 1103 associates/attaches the generated normal reproduction ECMs with/to the scrambled content to produce a TS and broadcasts the TS.

(Constructions of Reception Apparatus and Security Module)

[0294] The reception apparatus shown in FIG. 37 is made up of a TS separation unit 1201, a key changing judgement unit 1202, a key update judgement unit 1203, an HDD 1204, a scrambling key list generation unit 1205, a scrambling key list holding unit 1206, a descrambling process unit 1207, and a reproduction unit 205.
[0295] The security module shown in FIG. 37 is made up of an ECM interpretation unit 1301.
[0296] The TS separation unit 1201 receives a TS broadcast by the multiplexing unit 1103, and separates normal reproduction ECMs and scrambled content.

[0297] Here, scrambling keys are classified into even number keys and odd number keys.

[0298] FIG. 38 is a schematic diagram showing changes in the scrambling keys and timing for updating normal reproduction ECMs.

[0299] As shown in FIG. 38, one normal reproduction ECM transmits an even number key and an odd number key. When updating the normal reproduction ECM, either odd number key or even number key, which is not being used, is updated. Therefore, changes in the scrambling keys can be detected by the timing of changes between odd number keys and even number keys.

[0300] FIG. 39 is a schematic diagram showing changes between an even number key and an odd number key, and timing for updating normal reproduction ECMs. The scrambling control flag (note here that this term equals "transport scrambling control" prescribed in the MPEG-2 standard) shown in FIG. 39 is described in the TS packet header, which shows the state of the scrambling of the corresponding TS packet as follows. That is, in the case that the flag value is "00", scrambling is not performed, in the case of the flag value is "10", scrambling is performed using an even number key, and in the case that the flag value is "11", scrambling is performed using an odd number key.

[0301] As shown in FIG. 39, timing for changes between even number keys and odd number keys can be detected by change in the flag value of the scrambling control flag (① and ③ in FIG. 39). The timing for updating of normal reproduction ECMs can be detected by the version number of the normal reproduction ECMs (② in FIG. 39).

[0302] The key changing judgement unit 1202 counts the TS packet index indicating the ordinal position of the TS packet received by the TS separation unit 1201. The key changing judgement unit 1202 also checks the scrambling control flag in the TS packet header to judge whether the scrambling is performed by an even number key or an odd number key so as to detect the timing for changing in scrambling keys and the timing for ending of the storage.

[0303] The key update judgement unit 1203, firstly, has the HDD 1204 store the normal reproduction ECM separated by the TS separation unit 1201 therein. Each time a normal reproduction ECM is newly separated, the key update judgement unit 1203 judges whether the new normal reproduction ECM is the same as the stored normal reproduction ECM. In the case that they are not the same with each other, the key update judgement unit 1203 has the HDD 1204 overwrite the normal reproduction ECM stored in the HDD 1204 with the new normal reproduction ECM.

[0304] The HDD 1204 is a recording medium such as a hard disk drive. The HDD 1204 stores the scrambled content separated by the TS separation unit 1201 and the normal reproduction ECM passed by the key update judgement unit 1203.

[0305] The ECM interpretation unit 1301, at the timing for changing scrambling keys detected by the key changing judgement unit 1202, extracts the scrambling key that has been used until now and the scrambling key that will be used from now on, from the normal reproduction ECM stored in the HDD 1204, based on the judgement by the key changing judgement unit 1202, and passes the scrambling keys to the scrambling key list generation unit 1205.

[0306] The scrambling key list generation unit 1205 generates a scrambling key list, based on the TS packet index passed from the key changing judgement unit 1202 and the scrambling keys passed from the ECM interpretation unit 1301.

[0307] Following describes the processes for monitoring changes in scrambling keys and for generating the scrambling key list in detail.

[0308] FIG. 40 shows a transition of the scrambling key list generated.

[0309] As shown in FIG. 40, the scrambling key list is not updated at the timing of updating a normal reproduction ECM (② in FIG. 39), but underlined information shown in this figure is added thereto at the timing of changes between odd number keys and even number keys (① and ③ in FIG. 39).

[0310] The scrambling key list holding unit 1206 holds the scrambling key list generated by the scrambling key list generation unit 1205.

[0311] The descrambling process unit 1207 descrambles the scrambled content stored in the HDD 1204, based on the scrambling key list held by the scrambling key list holding unit 1206, and passes the descrambled content to the reproduction unit 205.

[0312] FIG. 41 shows the detailed construction of the descrambling unit 1207.

[0313] The descrambling process unit 1207 shown in FIG. 41 is made up of a TS packet extraction unit 1210, a descrambling unit 1211, and a scrambling key list interpretation unit 121.

[0314] The TS packet extraction unit 1210 extracts the scrambled content stored in the HDD 1204 one TS packet at a time, and passes the extracted content to the descrambling unit 1211. The TS packet extraction unit 1210 also counts the TS packet index indicating the ordinal position of the extracted TS packet counted from the beginning of the content, and passes the TS packet index to the scrambling key list interpretation unit 1212. The TS packet extraction unit 1210 resets the TS packet index into zero when other content starts to be processed.

[0315] The scrambling key list interpretation unit 1212 extracts the scrambling key corresponding to the TS packet index passed from the TS packet extraction unit 1210, from the scrambling key list held by the scrambling key list holding unit 1204, and passes the extracted key to the descrambling unit 1211.

[0316] The descrambling unit 1211 descrambles one TS packet passed from the TS packet extraction unit 1210 using the scrambling key extracted by the scrambling key list interpretation unit 1212, and passes the de-

scrambled TS packet to the reproduction unit 205. The descrambling unit 1211 repeats this process until all TS packets have been processed.

<Operations>

(Operations of Broadcast Apparatus)

[0317] FIG. 42 shows a procedure in the broadcasting process by means of the broadcast apparatus 1100 according to the fifth embodiment of the invention. Note that the same numerals are assigned to the step where the same processes as in FIG. 9 are conducted, and explanation for them has been omitted.

[0318] Following describes the outline of the procedure in the broadcast process, with reference to FIG. 42.

(1) Same as the step (1) in FIG. 9 (Step S1)
(2) Same as the step (2) in FIG. 9 (Step S2)
(3) Same as the step (3) in FIG. 9 (Step S3)
(4) The scrambling process unit 1101 scrambles the content converted into TS packets by the TS packetizing unit 101, based on the scrambling key acquired by the scrambling key acquisition unit 107 (Step S141).
(5) The ECM generation unit 1102 generates a normal reproduction ECM including the scrambling key acquired by the scrambling key acquisition unit 107 (Step S142).
(6) The multiplexing unit 1103 associates/attaches the generated normal reproduction ECM with/to the scrambled content to produce a TS and broadcasts the TS (Step S143).

(Operations of Reception Apparatus)

[0319] FIG. 43 shows a procedure in the reception and storage processes by means of the reception apparatus 1200 and the security module 1300 according to the fourth embodiment of the invention.

[0320] Following describes the outline of the procedure in the reception and storage processes, with reference to FIG. 43.

(1) The TS separation unit 1201 receives the first TS packet broadcast by the multiplexing unit 1103, and separates a normal reproduction ECM and scrambled content (Step S151).
(2) The key update judgement unit 1203 has the HDD 1204 store the normal reproduction ECM of the first TS packet separated by the TS separation unit 1201 therein (Step S152).
(3) The key changing judgement unit 1202 judges whether or not to complete the reception and storage processes (Step S153).
(4) If the reception and storage processes should not be completed, the TS separation unit 121 receives the following one TS packet broadcast by the multiplexing unit 1103, and separates a normal reproduction ECM and scrambled content (Step S154).
(5) The HDD 1204 stores the scrambled content separated by the TS separation unit 1201 (Step S155).
(6) The key changing judgement unit 1202 counts the TS packet index indicating the ordinal position of the TS packet received by the TS separation unit 1201. The key changing judgement unit 1202 also checks the scrambling control flag in the TS packet header to judge whether the scrambling is performed by an even number key or an odd number key (Step S156).
(7) The key changing judgement unit 1202 judges whether it is the timing for changing scrambling keys or not (Step S157).
(8) If it is the timing for changing scrambling keys, the key changing judgement unit 1202 passes the counted TS packet index to the scrambling key list generation unit 1205 (Step S158).
(9) The ECM interpretation unit 1301 extracts the scrambling key extracts the scrambling key that has been used until now and the scrambling key that will be used from now on, from the normal reproduction ECM stored in the HDD 1204, based on the judgement by the key changing judgement unit 1202, and passes the scrambling keys to the scrambling key list generation unit 1205 (Step S159).
(10) The scrambling key list generation unit 1205 updates the scrambling key list, based on the TS packet index passed from the key changing judgement unit 1202 and the scrambling keys passed from the ECM interpretation unit 1301 (Step S1510).
(11) The key update judgement unit 1203 judges whether the normal reproduction ECM separated by the TS separation unit 1202 is the same as the stored normal reproduction ECM (Step S1511). If they are the same with each other, the procedure returns upward (to Step S153) to process the successive TS packet (Step S1512).
(12) If they are not the same with each other, the key update judgement unit 1203 has the HDD 1204 overwrite the normal storage ECM stored therein with the new normal reproduction ECM. Then, the procedure returns upward (to Step S153) to process the successive TS packet (Step S1512)
(13) If the reception and storage processes should be completed, the key changing judgement unit 1202 passes the counted TS packet index to the scrambling key list generation unit 1205 (Step S1513).
(14) The scrambling key list generation unit 1205 updates the scrambling key list, based on the TS packet index passed from the key changing judgement unit 1202 to complete the scrambling key list (Step S1514).
(15) The scrambling key list holding unit 1206 holds the scrambling key list generated by the scrambling key list generation unit 1205 (Step S1515).

[0321] In the case that the reception and storage processes are completed without any changes in scrambling keys, the ECM interpretation unit 1301 extracts the scrambling key that has been used until now from the normal reproduction ECM stored in the HDD 1204, based on the judgement by the key changing judgement unit 1202, and passes the extracted key to the scrambling key list generation unit 1205. Then, the scrambling key list generation unit 1205 updates the scrambling key list, based on the TS packet index passed from the key changing judgement unit 1202 and the scrambling key passed from the ECM interpretation unit 1301 to complete the scrambling key list.

[0322] In addition, instead of separating normal reproduction ECM and scrambled content from each other when receiving them, but they may be separated before using to generate the scrambling key list.

[0323] FIG. 44 shows a procedure in the reproduction process after the reception and storage processes by means of the reception apparatus 1200 and the security module 1300 according to the fifth embodiment of the invention. Note that the same numerals are assigned to the step where the same processes as in FIG. 12 are conducted, and explanation for them has been omitted.

[0324] Following describes the outline of the procedure in the reproduction process, with reference to FIG. 44.

(1) The descrambling process unit 1205 descrambles the scrambled content stored in the HDD 1204, based on the scrambling key list held by the scrambling key list holding unit 1206, and passes the descrambled content to the reproduction unit 205 (Step S161).

(2) Same as the step (4) in FIG. 12 (Step S34)

[0325] FIG. 45 shows a procedure in the descrambling process by means of the descrambling process unit 1207 in detail.

[0326] Following describes the outline of the detailed procedure in the descrambling process, with reference to FIG. 45.

(1) The TS packet extraction unit 1210 resets the TS packet index into zero when other content starts to be processed (Step S171).

(2) The TS packet extraction unit 1210 judges whether there are unprocessed TS packets or not (Step S172). If there are not any unprocessed TS packet, the descrambling process ends.

(3) If there are unprocessed TS packets, the TS packet extraction unit 1210 extracts one unprocessed TS packet to pass it to the descrambling unit 1211. Also, the TS packet extraction unit 1210 counts the TS packet index to pass it to the scrambling key list interpretation unit 1212 (Step S173).

(4) The scrambling key list interpretation unit 1212 extracts the scrambling key corresponding to the TS packet index passed from the TS packet extraction unit 1210, from the scrambling key list held by the scrambling key list holding unit 1204 and passes the extracted key to the descrambling unit 1211 (Step S174).

(5) The descrambling unit 1211 descrambles one TS packet passed from the TS packet extraction unit 1210 using the scrambling key extracted by the scrambling key list interpretation unit 1212 and passes the descrambled TS packet to the reproduction unit 205. Then, the procedure returns upward to process the successive TS packet (Step S175).

[0327] In the fifth embodiment, in the case that a user has not made a contract to receive the content before receiving the content, the generated scrambling key list may be encoded and recorded, and after making the contract the list can be decoded so as to be used. Alternatively, instead of generating the scrambling key list, all normal reproduction ECMs may be stored when receiving the content, and then, after making the contract, the ECM interpretation unit 1001 may generate the scrambling key list from all the normal reproduction ECMs.

[0328] As described above, according to the fifth embodiment of the invention, various particular reproduction processes can be realized by extracting a scrambling key corresponding to any one of TS packets from the scrambling key list generated when/after storing scrambled content or the like.

[0329] Further, in order to improve the speed of the particular reproduction processes realized by selectively reproducing I pictures only, the I picture as a target may be extracted based on an I picture list, where the I picture list is generated in the same manner for generating the scrambling key list in the above-described embodiments.

[0330] The I picture list is represented by an I picture list descriptor, for example.

[0331] FIG. 46 shows one example of the data structure of an I picture list descriptor.

[0332] The I picture list descriptor shown in FIG. 46 includes an I picture identifier (Ipic_id) for identifying I pictures, the number of TS packets counted from the beginning of the file which indicates the position of the first packet of the I picture (first_packet_position), and the number of TS packets counted form the beginning of the file which indicates the position of the last packet of the I picture (last_packet_position). In the list, the I picture identifiers (Ipic_id), the number of TS packets (first_packet_position), and the number of TS packets (last_packet_position) are described as much as the number of I pictures.

(Modifications)

[0333] In some of the above-described embodiments, the scrambling key list is delivered by the same route as that for the scrambled content. However, the scrambling key list may be delivered by another route, for example,

by recording the list onto recording media such as a CD-ROM and delivering the recording media, or by means of another communication method such as the Internet and telephone.

[0334] In some of the above-described embodiments, the TS packet corresponding to the scrambling key is specified based on the number of TS packets. However, the TS packet may be specified by another method. For example, this may be based on the cumulative amount of data in the TS packet, a relative reproduction time from the beginning of the content. Alternatively, the TS packet may be specified by an identifier for the scrambling key, which is embedded for each TS packet in advance.

[0335] In each of the above-described embodiments, the scrambling keys are acquired from the database in the broadcast station. However, the scrambling keys may be generated before scrambling process.

[0336] Each of the above-described embodiments does not especially limit the timing for generating the scrambling key list. For instance, at the side of the broadcast apparatus, the list may be generated before scrambling, at the time of scrambling, or after scrambling. At the side of the reception apparatus, the list may be generated at any time before using the list in the descrambling process.

[0337] Besides, computer programs to have a computer execute the procedure of the above-described embodiments may be recorded on computer-readable recording media or may be directly transferred on the network to be distributed and sold.

[0338] These recording media can be, for example, removable recording media such as a floppy disk, a compact disk, a magnet optical disk, a DVD disk, and a memory card and fixed recording media such as hard disk, semiconductor memory.

[0339] Although the present invention has been fully described by way of examples with reference to the accompanying drawings, it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless such changes and modifications depart from the scope of the present invention, they should be construed as being included therein.

Claims

1. A reception apparatus (200) for receiving and reproducing scrambled content, comprising:

   reception means (201) for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content
   storage means (202) for storing the received scrambled content;
   descramble processing means (204) for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, and (b) obtaining a predetermined unit of content from the extracted predetermined unit of scrambled content; and
   reproduction means (205) for reproducing the predetermined unit of content in the obtained order, **characterised in that:**

   the reception means (201) are arranged to receive at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content is embedded,
   the storage means (202) are arranged to store the received storage information,
   the reception apparatus (200) further comprises list extraction means (301) for extracting the list from the stored storage information, and
   the descramble processing means (204) are arranged to extract a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list, and obtain the predetermined unit of content by descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

2. The reception apparatus of Claim 1, wherein
   the reception means (201) receives one piece of storage information in which the list is embedded,
   the storage means (202) stores the received scrambled content and the one piece of storage information, and
   the list extraction means (301) extracts the list from the stored one piece of storage information.

3. The reception apparatus of Claim 1, wherein the reception means (201) receives a plurality of pieces of storage information in each piece of which a divided portion of the list is embedded,
   the storage means (202) stores the received scrambled content and the plurality of pieces of storage information, and
   the list extraction means (3010 extracts the list from the stored plurality of pieces of storage information.

4. The reception apparatus of Claim 1, wherein the reception means (201) sequentially receives a transport stream (TS) packet including the predetermined unit of scrambled content,
   the storage means (202) sequentially stores the received TS packet, wherein
   the descramble processing means (204) includes:

   scrambled content extraction means for extract-

ing the predetermined unit of scrambled content from on of the TS packets stored in the storage means, and counting the ordinal position of the TS packet from the leading TS packet;
descrambling key extraction means (212) for extracting a descrambling key from the list, based on the counted ordinal position; and
descrambling means (211) for descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

5. The reception apparatus of Claim 1, wherein
the reception means (201) receives at least one storage Entitlement Control Message (ECM) as the at least one piece of storage information, the list being embedded in a portion to be encoded in the main body of the ECM,
the storage means (202) stores the received storage ECMs, and
the list extraction means (301) interprets the stored storage ECMs to extract the list.

6. The reception apparatus of Claim 5, wherein
the reception means (201) receives the storage ECMs including identifying information for distinguishing the storage ECMs from another type of ECM.

7. The reception apparatus of Claim 5, wherein
the reception means (201) receives the storage ECMs at a time.

8. The reception apparatus of Claim 1, wherein
the reception means (201) sequentially receives a TS packet including (a) the predetermined unit of scrambled content and (b) packet specifying information for specifying an unscrambled TS packet, and
the storage means (202) sequentially stores the received TS packet, wherein
the descramble processing means (204) includes:

scrambled content extraction means for extracting the predetermined unit of scrambled content and the packet specifying information from one of the TS packets stored in the storage means;
descrambling key extraction means (212) for extracting a descrambling key from the list, based on the extracted packet specifying information; and
descrambling means (211) for descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

9. The reception apparatus of Claim 8, wherein
the packet specifying information is one of Continuity Counter (CC), the number of TS packets, a cumulative amount of data, a relative reproduction time, and a scrambling key identifier,
the scrambled content extraction means (210) extracts, as the packet specifying information, one of the Continuity Counter (CC), the number of TS packets, the cumulative amount of data, the relative reproduction time, and the scrambling key identifier, and
the descrambling key extraction means (212) performs a predetermined operation to the extracted information as the packet identifying information to generate a descrabling key identifier, and extracts a descrambling key from the list based on the descrambling key identifier.

10. The reception apparatus of Claim 1, wherein
the reception means (201) sequentially receives a TS packet including (a) the predetermined unit of scrambled content and (b) unscrambled I picture information, wherein the I picture information indicates whether the TS packet corresponding to the information consists of a portion of an I picture/an I picture or not, and
the storage means (202) sequentially stores the received TS packet, wherein
the descramble processing means (204) includes:

scrambled content extraction means (210) for, when performing particular reproduction processes, extracting the predetermined unit of scrambled content and I picture information from one of the TS packets stored in the storage means;
I picture judgement means (204, S52) for judging whether the extracted predetermined unit of scrambled content consists of a portion of an I picture/an I picture or not, based on the extracted I picture information;
descrambling key extraction means (212) for extracting a descrambling key from the list, only when the extracted predetermined unit of scrambled content consists of a portion of an I picture/an I picture; and
descrambling means (211) for descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

11. The reception apparatus of Claim 1 further managing contract information and consisting of a security module whose portion does not effectively function if a contract has not been made, and other modules, the reception apparatus further comprising:

list holding means (203) for holding the list extracted by the list extraction means,

wherein the list extraction means (301) and the list holding means (203) are provided within the security module.

12. A broadcast apparatus (100) for scrambling content and broadcasting the scrambled content to a reception apparatus (200), the broadcast apparatus (100) comprising:

acquisition means (106, 107) for acquiring content to be scrambled and a plurality of descrambling keys;
scramble processing means (103) for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and
broadcast means (105) is arranged to broadcast the scrambled content, **characterised in that**;
the broadcast apparatus (100) further comprises: list generation means (102) for generating a list of the descrambling keys; and embedding means (104) for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information, and
the broadcast means (105) is arranged to broadcast the generated storage information.

13. The broadcast apparatus of Claim 12, wherein
the embedding means (104) embeds the list in one piece of predetermined information to generate one piece of storage information, and
the broadcast means (105) broadcasts the generated one piece of information and the scrambled content.

14. The broadcast apparatus of claim 12, wherein
the embedding means embeds a divided portion of the list in each of a plurality of pieces of predetermined information to generate a plurality of pieces of storage information, and
the broadcast means (105) broadcasts the generated plurality of pieces of storage information and the scrambled content.

15. The broadcast apparatus of claim 12, wherein
the embedding means (104) embeds the list in a portion to be encoded in a main body of at least one ECM to generate at least one piece of storage information.

16. The broadcast apparatus of Claim 12, wherein
the broadcast means (105) broadcasts one set of the storage information while all the scrambled content corresponding descrambled order.

17. A computer program comprising computer code to, when loaded into a computer system and executed, cause said computer system to perform the following steps:

a reception step (S21) for receiving scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content;
a storage step (S22) for storing the received scrambled content;
a descramble processing step (S33) for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, and (b) obtaining a predetermined unit of content from the extracted predetermined unit of scrambled content; and
a reproduction step (S34) for reproducing the predetermined unit of content in the obtained order, **characterised in that:**

the reception step (S21) is further for receiving at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content is embedded,
the storage step (S22) is further for storing the received storage information,
the computer code further causes said computer system to perform a list extraction step (S31) for extracting the list from the stored storage information, and
the descramble processing step (S33) is further for extracting a descrambling key corresponding to the predetermined unit of scrambled content from the extracted list, and for obtaining the predetermined unit of content by descrambling the extracted predetermined unit of scrambled content using the extracted descrambling key.

18. A computer program comprising computer code to, when loaded into a computer system and executed, cause said computer system to perform the following steps:

an acquisition step (S1, S3) for acquiring for acquiring content to be scrambled and a plurality of descrambling keys;
a scramble processing step (S5) for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and
a broadcast step (S7) for broadcasting the scrambled content, **characterised in that:**

the computer code further causes said computer system to perform: a list generation step (S4) for generating a list of the descrambling keys; and an embedding step (S6) for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information, and
the broadcast step (S7) is further for broadcasting the generated storage information.

19. A recording medium for storing instructions which cause at least a portion of a computer system to perform the following steps:

a reception step (S21) for receiving scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content,
a storage step (S22) for storing the received scrambled content;
a descramble processing step (S33) for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, and (b) obtaining a predetermined unit of content from the extracted predetermined unit of scrambled content; and
a reproduction step (S34) for reproducing the predetermined unit of content in the obtained order,

characterised in that:

the reception step (S21) is further for receiving at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content is embedded,
the storage step (S22) is further for storing the received storage information, and
the instructions further cause said computer system to perform a list extraction step (S31) for extracting the list from the stored storage information.

20. A recording medium for storing instructions which cause at least a portion of a computer system to perform the following steps:

an acquisition step (S1,S3) for acquiring content to be scrambled and a plurality of descrambling keys;
a scramble processing step (S5) for scrambling a predetermined unit of content out of the acquired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and
a broadcast step (S7) for broadcasting the scrambled content **characterised in that:**

the instructions further cause said computer system to perform: a list generation step (S4) for generating a list of the descrambling keys; and an embedding step(S6) for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information, and
the broadcast step (S7) is further for broadcasting the generated storage information.

21. A method for receiving and reproducing scrambled content, the method comprising the steps of:

a reception step (S21) for receiving the scrambled content, wherein the scrambled content is scrambled so that a predetermined unit of scrambled content, which is a portion of the scrambled content, is descrambled using a descrambling key corresponding to the predetermined unit of scrambled content;
a storage step (S22) for storing the received scrambled content;
a descramble processing step (S33) for (a) extracting the predetermined unit of scrambled content from the stored scrambled content, and (b) obtaining a predetermined unit of content from the extracted predetermined unit of scrambled content; and
a reproduction step (S34) for reproducing the predetermined unit of content in the obtained order, **characterised in that**
the reception step (S21) is further for receiving at least one piece of storage information in which a list including all descrambling keys to be used for descrambling the scrambled content is embedded,
the storage step (S22) is further for storing the received storage information, and
the method further comprises a list extraction step (S31) for extracting the list from the stored storage information.

22. A method for scrambling content and broadcasting the scrambled content to a reception apparatus (200), the method comprising the steps of:

an acquisition step (S1,S3) for acquiring content to be scrambled and a plurality of descrambling keys;
a scramble processing step (S5) for scrambling a predetermined unit of content out of the ac-

quired content so that the predetermined unit of scrambled content is descrambled using a descrambling key different for each predetermined unit or each set of a plurality of predetermined units; and
a broadcast step (S7) for broadcasting the scrambled content, **characterised in that**:

the method further comprises: a list generation step (S4) for generating a list of the descrambling keys; and an embedding step (S6) for embedding the list in at least one piece of predetermined information to generate at least one piece of storage information, and
the broadcast step (S7) is further for broadcasting the generated storage information.

Patentansprüche

1. Empfangsvorrichtung (200) zum Empfangen und Wiedergeben von verscrambeltem Inhalt, die umfasst:

eine Empfangseinrichtung (201), die den verscrambelten Inhalt empfängt, wobei der verscrambelte Inhalt so verscrambelt ist, dass eine vorgegebene Einheit von verscrambeltem Inhalt, die ein Teil des verscrambelten Inhalts ist, unter Verwendung eines Entscrambelungs-Schlüssels entsprechend der vorgegebenen Einheit von verscrambeltem Inhalt entscrambelt wird,
eine Speichereinrichtung (202), die den empfangenen verscrambelten Inhalt speichert;
eine Entscrambel-Verarbeitungseinrichtung (204), die (a) die vorgegebene Einheit von verscrambeltem Inhalt aus dem gespeicherten verscrambeltem Inhalt extrahiert, und (b) eine vorgegebene Einheit von Inhalt aus der extrahierten vorgegebenen Einheit von verscrambeltem Inhalt gewinnt; und
eine Wiedergabeeinrichtung (205), die die vorgegebene Einheit von Inhalt in der gewonnenen Reihenfolge wiedergibt, **dadurch gekennzeichnet, dass**:

die Empfangseinrichtung (201) so eingerichtet ist, dass sie wenigstens ein Element von Speicherinformationen empfängt, in das eine Liste eingebettet ist, die alle zum Entscrambeln des verscrambelten Inhalts zu verwendenden Entscrambelungs-Schlüssel enthält,
die Speichereinrichtung (202) so eingerichtet ist, dass sie die empfangenen Speicherinformationen speichert,
die Empfangsvorrichtung (200) des Weiteren eine Listen-Extrahiereinrichtung (301) umfasst, die die Liste aus den gespeicherten Speicherinformationen extrahiert, und
die Entscrambel-Verarbeitungseinrichtung (204) so eingerichtet ist, dass sie einen Entscrambelungs-Schlüssel entsprechend der vorgegebenen Einheit von verscrambeltem Inhalt, aus der extrahierten Liste extrahiert, und die vorgegebene Einheit von Inhalt gewinnt, indem sie die extrahierte vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung des extrahierten Entscrambelungs-Schlüssels gewinnt.

2. Empfangsvorrichtung nach Anspruch 1, wobei
die Empfangseinrichtung (201) ein Element von Speicherinformationen empfängt, in das die Liste eingebettet ist,
die Speichereinrichtung (202) den empfangenen verscrambelten Inhalt und das eine Element von Speicherinformationen speichert, und
die Listen-Extrahiereinrichtung (301) die Liste aus dem gespeicherten einen Element von Speicherinformationen extrahiert.

3. Empfangsvorrichtung nach Anspruch 1, wobei die Empfangseinrichtung (201) eine Vielzahl von Elementen von Speicherinformationen empfängt, und wobei in jedem Element derselben ein separater Teil der Liste eingebettet ist,
die Speichereinrichtung (202) den empfangenen verscrambelten Inhalt und die Vielzahl von Elementen von Speicherinformationen speichert, und
die Listen-Extrahiereinrichtung (301) die Liste aus der gespeicherten Vielzahl von Elementen von Speicherinformationen extrahiert.

4. Empfangsvorrichtung nach Anspruch 1, wobei die Empfangseinrichtung (201) sequenziell ein Transportstrom (TS)-Paket empfängt, das die vorgegebene Einheit von verscrambeltem Inhalt enthält,
die Speichereinrichtung (202) sequenziell das empfangene Transportstrom-Paket speichert, wobei die Entscrambel-Verarbeitungseinrichtung (204) enthält:

eine Einrichtung zum Extrahieren von verscrambeltem Inhalt, die die vorgegebene Einheit von verscrambeltem Inhalt aus einem der in der Speichereinrichtung gespeicherten Transportstrom-Pakete extrahiert und die Ordinalposition des Transportstrom-Paketes von dem vorderen Transportstrom-Paket an zählt;
eine Einrichtung (212) zum Extrahieren eines Entscrambelungs-Schlüssels, die auf Basis der gezählten Ordinalposition einen Entscrambelungs-Schlüssel aus der Liste extrahiert; und

eine Entscrambelungs-Einrichtung (211), die die extrahierte vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung des extrahierten Entscrambelungs-Schlüssels entscrambelt.

5. Empfangsvorrichtung nach Anspruch 1, wobei die Empfangseinrichtung (201) wenigstens eine Speicher-Berechtigungsmitteilung (Entitlement Controll Message - ECM) als das wenigstens eine Element von Speicherinformationen empfängt, wobei die Liste in einen zu codierenden Abschnitt in dem Hauptkörper der ECM eingebettet ist,
die Speichereinrichtung (202) die empfangenen Speicher-ECM speichert; und
die Listen-Extrahiereinrichtung (301) die gespeicherten Speicher-ECM interpretiert, um die Liste zu extrahieren.

6. Empfangsvorrichtung nach Anspruch 5, wobei die Empfangseinrichtung (201) die Speicher-ECM empfängt, die Identifizierungsinformationen enthalten, um die Speicher-ECM von ECM eines anderen Typs zu unterscheiden.

7. Empfangsvorrichtung nach Anspruch 5, wobei die Empfangseinrichtung (201) die Speicher-ECM einzeln empfängt.

8. Empfangsvorrichtung nach Anspruch 1, wobei die Empfangseinrichtung (201) sequenziell ein Transportstrom-Paket empfängt, das (a) die vorgegebene Einheit von verscrambeltem Inhalt, und (b) Paket-Spezifizierungsinformationen enthält, die ein nicht-verscrambeltes Transportstrom-Paket spezifizieren, und
die Speichereinrichtung (202) sequenziell das empfangene Transportstrom-Paket speichert, wobei die Entscrambel-Verarbeitungseinrichtung (204) enthält:

eine Einrichtung zum Extrahieren von verscrambeltem Inhalt, die die vorgegebene Einheit von verscrambeltem Inhalt und die Paket-Spezifizierungsinformationen aus einem der in der Speichereinrichtung gespeicherten Transportstrom-Pakete extrahiert;
eine Einrichtung (212) zum Extrahieren eines Entscrambelungs-Schlüssels, die einen Entscrambelungs-Schlüssel auf Basis der extrahierten Paket-Spezifizierungsinformationen aus der Liste extrahiert; und
eine Entscrambelungs-Einrichtung (211), die die extrahierte vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung des extrahierten Entscrambelungs-Schlüssels entscrambelt.

9. Empfangsvorrichtung nach Anspruch 8, wobei die Paket-Spezifizierungsinformationen ein Zähler (Continuity Counter - CC) ist, die Anzahl von Transportstrom-Paketen, eine kumulative Menge an Daten, eine relative Wiedergabezeit oder eine Verscrambelungs-Schlüssel-Kennung ist,
die Einrichtung (210) zum Extrahieren von verscrambeltem Inhalt als die Paket-Spezifizierungsinformationen den Zähler (CC), die Anzahl von Transportstrom-Paketen, die kumulative Menge an Daten, die relative Wiedergabezeit oder die Verscrambelungs-Schlüssel-Kennung extrahiert, und
die Einrichtung (212) zum Extrahieren eines Entscrambelungs-Schlüssels eine vorgegebene Operation an den extrahierten Informationen als den Paket-Identifizierungsinformationen durchführt, um eine Entscrambelungs-Schlüssel-Kennung zu erzeugen, und einen Entscrambelungs-Schlüssel auf Basis der Entscrambelungs-Schlüssel-Kennung aus der Liste extrahiert.

10. Empfangsvorrichtung nach Anspruch 1, wobei die Empfangseinrichtung (201) sequenziell ein Transportstrom-Paket empfängt, das (a) die vorgegebene Einheit von verscrambeltem Inhalt und (b) nicht-verscrambelte I-Bild-Informationen enthält, wobei die I-Bild-Informationen anzeigen, ob das den Informationen entsprechende Transportstrom-Paket aus einem Teil eines I-Bildes/einem I-Bild besteht oder nicht, und
die Speichereinrichtung (202) sequenziell das empfangene Transportstrom-Paket speichert, wobei die Entscrambel-Verarbeitungseinrichtung (204) enthält:

eine Einrichtung (210) zum Extrahieren von verscrambeltem Inhalt, die, wenn sie bestimmte Wiedergabeprozesse durchführt, die vorgegebene Einheit von verscrambeltem Inhalt und I-Bild-Informationen aus einem der in der Speichereinrichtung gespeicherten Transportstrom-Pakete extrahiert;
eine I-Bild-Feststelleinrichtung (204, S52), die auf Basis der extrahierten I-Bild-Informationen feststellt, ob die extrahierte vorgegebene Einheit von verscrambeltem Inhalt aus einem Teil eines I-Bildes/einem I-Bild besteht oder nicht;
eine Einrichtung (212) zum Extrahieren eines Entscrambelungs-Schlüssels, die einen Entscrambelungs-Schlüssel aus der Liste nur dann extrahiert, wenn die extrahierte vorgegebene Einheit von verscrambeltem Inhalt aus einem Teil eines I-Bildes/einem I-Bild besteht; und
eine Entscrambelungs-Einrichtung (211), die die extrahierte vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung des extrahierten Entscrambelungs-Schlüssels entscrambelt.

11. Empfangsvorrichtung nach Anspruch 1, die des Weiteren Vertrags-Informationen verwaltet und aus einem Sicherheitsmodul, dessen Teil nicht effektiv funktioniert, wenn kein Vertrag geschlossen worden ist, sowie aus anderen Modulen besteht, wobei die Empfangsvorrichtung des Weiteren umfasst:

eine Listen-Speichereinrichtung (203), die die durch die Listen-Extrahiereinrichtung extrahierte Liste speichert,

wobei die Listen-Extrahiereinrichtung (301) und die Listen-Speichereinrichtung (203) in dem Sicherheitsmodul vorhanden sind.

12. Rundsendevorrichtung (100), die Inhalt verscrambelt und den verscrambelten Inhalt zu einer Empfangsvorrichtung (200) rundsendet, wobei die Rundsendevorrichtung (100) umfasst:

eine Erfassungseinrichtung (106, 107), die zu verscrambelnden Inhalt und eine Vielzahl von Entscrambelungs-Schlüsseln erfasst;
eine Verscrambelungs-Verarbeitungseinrichtung (103), die eine vorgegebene Einheit von Inhalt aus dem erfassten Inhalt verscrambelt, so dass die vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung eines Entscrambelungs-Schlüssels entscrambelt wird, der für jede vorgegebene Einheit oder jede Gruppe einer Vielzahl vorgegebener Einheiten verschieden ist; und
eine Rundsendeeinrichtung (105), die so eingerichtet ist, dass sie den verscrambelten Inhalt rundsendet,

dadurch gekennzeichnet, dass
die Rundsendevorrichtung (100) des Weiteren umfasst:

eine Listen-Erzeugungseinrichtung (102), die eine Liste der Entscrambelungs-Schlüssel erzeugt, und eine Einbetteinrichtung (104), die die Liste in wenigstens ein Element vorgegebener Informationen einbettet, um wenigstens ein Element von Speicherinformationen zu erzeugen, und
die Rundsendeeinrichtung (105) so eingerichtet ist, dass sie die erzeugten Speicherinformationen rundsendet.

13. Rundsendevorrichtung nach Anspruch 12, wobei die Einbetteinrichtung (104) die Liste in ein Element vorgegebener Informationen einbettet, um ein Element von Speicherinformationen zu erzeugen, und die Rundsendeeinrichtung (105) das erzeugte eine Element von Informationen und den verscrambelten Inhalt rundsendet..

14. Rundsendevorrichtung nach Anspruch 12, wobei die Einbetteinrichtung einen separaten Teil der Liste in jedes einer Vielzahl von Elementen vorgegebener Informationen einbettet, um eine Vielzahl von Elementen von Speicherinformationen zu erzeugen, und
die Rundsendeeinrichtung (105) die erzeugte Vielzahl von Elementen von Speicherinformationen und den verscrambelten Inhalt rundsendet.

15. Rundsendevorrichtung nach Anspruch 12, wobei die Einbetteinrichtung (104) die Liste in einem zu codierenden Teil in einem Hauptkörper wenigstens einer ECM einbettet, um wenigstens ein Element von Speicherinformationen zu erzeugen.

16. Rundsendevorrichtung nach Anspruch 12, wobei die Rundsendeeinrichtung (105) eine Gruppe der Speicherinformationen rundsendet und der gesamte verscrambelte Inhalt der Entscrambelungs-Reihenfolge entspricht.

17. Computerprogramm, das Computercode umfasst, der, wenn er in ein Computersystem geladen und ausgeführt wird, das Computersystem veranlasst, die folgenden Schritte durchzuführen.
einen Empfangsschritt (S21) zum Empfangen von verscrambeltem Inhalt, wobei der verscrambelte Inhalt so verscrambelt ist, dass eine vorgegebene Einheit von verscrambeltem Inhalt, die ein Teil des verscrambeltem Inhalt ist, unter Verwendung eines Entscrambelungs-Schlüssels entsprechend der vorgegebenen Einheit von verscrambeltem Inhalt entscrambelt wird;
einen Speicherschritt (S22) zum Speichern des empfangenen verscrambelten Inhalts;
einen Entscrambel-Verarbeitungsschritt (S33) zum (a) Extrahieren der vorgegebenen Einheit von verscrambeltem Inhalt aus dem gespeicherten verscrambelten Inhalt, und (b) Gewinnen einer vorgegebenen Einheit von Inhalt aus der extrahierten vorgegebenen Einheit von verscrambeltem Inhalt; und
einen Wiedergabeschritt (S34) zum Wiedergeben der vorgegebenen Einheit von Inhalt in der gewonnenen Reihenfolge, **dadurch gekennzeichnet, dass:**

der Empfangsschritt (S21) des Weiteren dazu dient, wenigstens ein Element von Speicherinformationen zu empfangen, in das eine Liste eingebettet ist, die alle zum Entscrambeln des verscrambelten Inhalts zu verwendenden Entscrambelungs-Schlüssel enthält,
der Speicherschritt (S22) des Weiteren dazu dient, die empfangenen Speicherinformationen zu speichern,
der Computercode das Computersystem des Weiteren veranlasst, einen Listen-Extrahier-

schritt (S31) zum Extrahieren der Liste aus den gespeicherten Speicherinformationen durchzuführen, und
der Entscrambelungs-Verarbeitungsschritt (S33) des Weiteren dazu dient, einen Entscrambelungs-Schlüssel entsprechend der vorgegebenen Einheit von verscrambeltem Inhalt aus der extrahierten Liste zu extrahieren und dazu, die vorgegebene Einheit von Inhalt durch Entscrambeln der extrahierten vorgegebenen Einheit von verscrambeltem Inhalt unter Verwendung des extrahierten Entscrambelungs-Schlüssels zu gewinnen.

18. Computerprogramm, das Computercode umfasst, der, wenn er in ein Computersystem geladen und ausgeführt wird, das Computersystem veranlasst, die folgenden Schritte durchzuführen:

einen Erfassungsschritt (S1, S3) zum Erfassen von zu verscrambelndem Erfassungsinhalt und einer Vielzahl von Entscrambelungs-Schlüsseln;
einen Verscrambel-Verarbeitungsschritt (S5) zum Verscrambeln einer vorgegebenen Einheit von Inhalt aus dem erfassten Inhalt, so dass die vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung eines Entscrambelungs-Schlüssels entscrambelt wird, der für jede vorgegebene Einheit oder jede Gruppe einer Vielzahl vorgegebener Einheiten verschieden ist; und
einen Rundsendeschritt (S7) zum Rundsenden des verscrambelten Inhalts, **dadurch gekennzeichnet, dass**
der Computercode das Computersystem des Weiteren veranlasst, durchzuführen:

einen Listen-Erzeugungsschritt (S4) zum Erzeugen einer Liste der Verscrambelungs-Schlüssel;
und einen Einbettschritt (S6) zum Einbetten der Liste in wenigstens ein Element vorgegebener Informationen, um wenigstens ein Element von Speicherinformationen zu erzeugen, und
der Rundsendeschritt (S7) des Weiteren zum Rundsenden der erzeugten Speicherinformationen dient.

19. Aufzeichnungsmedium zum Speichern von Befehlen, die wenigstens einen Abschnitt eines Computersystems veranlassen, die folgenden Schritte durchzuführen:

einen Empfangsschritt (S21) zum Empfangen von verscrambeltem Inhalt, wobei der verscrambelte Inhalt so verscrambelt wird, dass eine vorgegebene Einheit von verscrambeltem Inhalt, die ein Teil des verscrambelten Inhalts ist, unter Verwendung eines Entscrambelungs-Schlüssels entsprechend der vorgegebenen Einheit von verscrambeltem Inhalt entscrambelt wird,
einen Speicherschritt (S22) zum Speichern des empfangenen verscrambelten Inhalts;
einen Entscrambel-Verarbeitungsschritt (S33) zum (a) Extrahieren der vorgegebenen Einheit von verscrambeltem Inhalt aus dem gespeicherten verscrambelten Inhalt, und (b) Gewinnen einer vorgegebenen Einheit von Inhalt aus der extrahierten vorgegebenen Einheit von verscrambeltem Inhalt; und
einen Wiedergabeschritt (S34) zum Wiedergeben der vorgegebenen Einheit von Inhalt in der gewonnenen Reihenfolge,

dadurch gekennzeichnet, dass:

der Empfangsschritt (S21) des Weiteren dazu dient, wenigstens ein Element von Speicherinformationen zu empfangen, in das eine Liste eingebettet ist, die alle zum Entscrambeln des verscrambelten Inhalts zu verwendenden Entscrambelungs-Schlüssel enthält,
der Speicherschritt (S22) des Weiteren dazu dient, die empfangenen Speicherinformationen zu speichern, und
die Befehle das Computersystem des Weiteren veranlassen, einen Listen-Extrahierschritt (S31) zum Extrahieren der Liste aus den gespeicherten Speicherinformationen durchzuführen.

20. Aufzeichnungsmedium zum Speichern von Befehlen, die wenigstens einen Teil eines Computersystems veranlassen, die folgenden Schritte durchzuführen:

einen Erfassungsschritt (S1, S3) zum Erfassen von zu verscrambelndem Inhalt und einer Vielzahl von Entscrambelungs-Schlüsseln;
einen Verscrambel-Verarbeitungsschritt (S5) zum Verscrambeln einer vorgegebenen Einheit von Inhalt aus dem erfassten Inhalt, so dass die vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung eines Entscrambelungs-Schlüssels entscrambelt wird, der für jede vorgegebene Einheit oder jede Gruppe einer Vielzahl vorgegebener Einheiten verschieden ist; und
einen Rundsendeschritt (S7) zum Rundsenden des verscrambelten Inhalts, **dadurch gekennzeichnet, dass**:

die Befehle das Computersystem des Weiteren veranlassen, durchzuführen:

einen Listen-Erzeugungsschritt (S4) zum Erzeugen einer Liste der Entscrambelungs-Schlüssel; und
einen Einbettschritt (S6) zum Einbetten der Liste in wenigstens ein Element vorgegebener Informationen, um wenigstens ein Element von Speicherinformationen zu erzeugen, und
der Rundsendeschritt (S7) des Weiteren zum Rundsenden der erzeugten Speicherinformationen dient.

21. Verfahren zum Empfangen und Wiedergeben von verscrambeltem Inhalt, wobei das Verfahren die folgenden Schritte umfasst:

einen Empfangsschritt (S21) zum Empfangen des verscrambelten Inhalts, wobei der verscrambelte Inhalt so verscrambelt ist, dass eine vorgegebene Einheit von verscrambeltem Inhalt, die ein Teil des verscrambelten Inhalts ist, unter Verwendung eines Entscrambelungs-Schlüssels entsprechend der vorgegebenen Einheit von verscrambeltem Inhalt entscrambelt wird;
einen Speicherschritt (S22) zum Speichern des empfangenen verscrambelten Inhalts;
einen Entscrambel-Verarbeitungsschritt (S33) zum (a) Extrahieren der vorgegebenen Einheit von verscrambeltem Inhalt aus dem gespeicherten verscrambeltem Inhalt und (b) Gewinnen einer vorgegebenen Einheit von Inhalt aus der extrahierten vorgegebenen Einheit von verscrambeltem Inhalt; und
einen Wiedergabeschritt (S34) zum Wiedergeben der vorgegebenen Einheit von Inhalt in der gewonnenen Reihenfolge, **dadurch gekennzeichnet, dass**:

der Empfangsschritt (S21) des Weiteren dazu dient, wenigstens ein Element von Speicherinformationen zu empfangen, in das eine Liste eingebettet ist, die alle zum Entscrambeln des verscrambelten Inhalts zu verwendenden Entscrambelungs-Schlüssel enthält,
der Speicherschritt (S22) des Weiteren dazu dient, die empfangenen Speicherinformationen zu speichern, und
das Verfahren des Weiteren einen Listen-Extrahierschritt (S31) zum Extrahieren der Liste aus den gespeicherten Speicherinformationen umfasst.

22. Verfahren zum Verscrambeln von Inhalt und Rundsenden des verscrambelten Inhalts an eine Empfangsvorrichtung (200), wobei das Verfahren die folgenden Schritte umfasst:

einen Erfassungsschritt (S1, S3) zum Erfassen von zu verscrambelndem Inhalt und einer Vielzahl von Entscrambelungs-Schlüsseln;
einen Verscrambel-Verarbeitungsschritt (S5) zum Verscrambeln einer vorgegebenen Einheit vom Inhalt aus dem erfassten Inhalt, so dass die vorgegebene Einheit von verscrambeltem Inhalt unter Verwendung eines Entscrambelungs-Schlüssels entscrambelt wird, der für jede vorgegebene Einheit oder jede Gruppe einer Vielzahl vorgegebener Einheiten verschieden ist; und
einen Rundsendeschritt (S7) zum Rundsenden des verscrambelten Inhalts, **dadurch gekennzeichnet, dass**:

das Verfahren des Weiteren umfasst:

einen Listen-Erzeugungsschritt (S4) zum Erzeugen einer Liste der Entscrambelungs-Schlüssel; und einen Einbettschritt (S6) zum Einbetten der Liste in wenigstens ein Element vorgegebener Informationen, um wenigstens ein Element von Speicherinformationen zu erzeugen, und
der Rundsendeschritt (S7) des Weiteren zum Rundsenden der erzeugten Speicherinformationen dient.

Revendications

1. Dispositif de réception (200) pour recevoir et reproduire un contenu brouillé; comprenant :

des moyens de réception (201) pour recevoir le contenu brouillé, le contenu brouillé étant brouillé de telle sorte qu'une unité prédéterminée du contenu brouillé, qui est une partie du contenu brouillé, est désembrouillée moyennant l'utilisation d'une clé de désembrouillage correspondant à l'unité prédéterminée du contenu brouillé;
des moyens de mémoire (202) pour mémoriser le contenu brouillé reçu;
des moyens (204) de traitement de désembrouillage pour (a) extraire l'unité prédéterminée de contenu désembrouillé à partir du contenu brouillé mémorisé, et (b) obtenir une unité prédéterminée de contenu à partir de l'unité prédéterminée extraite de contenu brouillé; et
des moyens de reproduction (205) pour reproduire l'unité prédéterminée de contenu dans l'ordre obtenu,

caractérisé en ce que :

les moyens de réception (201) sont agencés de manière à recevoir au moins un élément de l'information de mémorisation, dans laquelle est insérée une liste incluant toutes les clés de déaembrouillage devant être utilisées pour désembrouiller le contenu brouillé,
les moyens de mémoire (202) sont agencés de manière à mémoriser l'information de mémoire reçue,
le dispositif de réception (200) comporte en outre des moyens (301) d'extraction de liste pour extraire la liste à partir de l'information de mémoire mémorisée, et
les moyens (204) de traitement de désembrouillage sont agencés pour l'extraction d'une clé de désembrouillage correspondant à l'unité prédéterminée de contenu brouillé à partir de la liste extraite, l'obtention de l'unité prédéterminée de contenu par désembrouillage de l'unité prédéterminée extraite de contenu brouillé en utilisant la clé de désembrouillage extraite.

2. Dispositif de réception selon la revendication 1, dans lequel
les moyens de réception (201) reçoivent un élément d'information de mémoire, dans lequel la liste est insérée,
les moyens de mémoire (202) mémorisent le contenu brouillé reçu et le un élément d'information de mémoire, et
les moyens d'extraction de liste (301) extraient la liste à partir d'un élément mémorisé de l'information de mémoire.

3. Dispositif de réception selon la revendication 1, dans lequel les moyens de réception (201) reçoivent une pluralité d'éléments d'information de mémoire dans chacun desquels est insérée une partie divisée de la liste,
les moyens de mémoire (202) mémorisent le contenu brouillé reçu et la pluralité d'éléments d'information de mémoire, et
les moyens (301) d'extraction de la liste extraient la liste à partir de la pluralité mémorisée d'éléments d'information de mémoire.

4. Dispositif de réception selon la revendication 1, dans lequel les moyens de réception (201) reçoivent séquentiellement un paquet de flux de transport (TS) incluant l'unité prédéterminée de contenu brouillé,
les moyens de mémoire (202) mémorisent séquentiellement le paquet de flux TS reçu, dans lequel
les moyens de traitement de désembrouillage (204) incluent :

des moyens d'extraction du contenu brouillé pour extraire l'unité prédéterminée du contenu brouillé à partir de l'un des paquets de flux TS mémorisés dans les moyens de mémoire, et compter la position ordinale des paquets de flux TS à partir du paquet de flux TS de tête;
des moyens (212) d'extraction de clé de désembrouillage pour extraire une clé de désembrouillage à partir de la liste, sur la base de la position ordinale comptée; et
des moyens de désembrouillage (211) pour désembrouiller l'unité prédéterminée extraite du contenu désembrouillé en utilisant la clé de désembrouillage extraite.

5. Dispositif de réception selon la revendication 1, dans lequel :

les moyens de réception (201) reçoivent au moins un message de commande d'intitulé en mémoire (ECM) en tant qu'au moins un élément de l'information de mémoire, la liste étant insérée dans une partie devant être codée dans le corps principal du message ECM,
les moyens de mémoire (202) mémorisent des messages ECM de mémoire reçus, et
des moyens (301) d'extraction de la liste interprètent des messages ECM de mémoire reçus, pour extraire la liste.

6. Dispositif de réception selon la revendication 5, dans lequel
les moyens de réception (201) reçoivent les messages ECM de mémoire incluant une information d'identification servant à distinguer les messages ECM de mémoire vis-à-vis d'un autre type de message ECM.

7. Dispositif de réception selon la revendication 5, dans lequel les moyens de réception (201) reçoivent les messages ECM de mémoire à un instant donné.

8. Dispositif de réception selon la revendication 1, dans lequel les moyens de réception (201) reçoivent séquentiellement un paquet de flux TS incluant (a) l'unité prédéterminée du contenu brouillé et (b) une information de spécification de paquet servant à spécifier un paquet de flux TS non brouillé, et
les moyens de mémoire (202) mémorisent séquentiellement le paquet de flux TS reçu,
dans lequel les moyens de traitement de désembrouillage (204) incluent :

des moyens d'extraction de contenu brouillé et l'information de spécification de paquet à partir de l'un des paquets de flux TS mémorisés dans les moyens de mémoire;
des moyens (212) d'extraction de clé de désembrouillage pour extraire une clé de désembrouillage à partir de la liste, sur la base de l'information de spécification de paquet extrait; et

des moyens de désembrouillage (211) pour désembrouiller l'unité prédéterminée extraite du contenu brouillé en utilisant la clé de désembrouillage extraite.

9. Dispositif de réception selon la revendication 8, dans lequel
l'information de spécification de paquet est l'un de compteur de continuité (CC), du nombre de paquets de flux TS, d'un nombre cumulé de données, d'une durée de reproduction relative et d'un identifiant de clé de brouillage,
les moyens (210) d'extraction du contenu brouillé extraient, en tant qu'information de spécification de paquets, l'un du compteur de continuité (CC), du nombre de paquets de flux TS, de la quantité cumulée de données, de la durée de reproduction relative et de l'identifiant de clé de brouillage, et
les moyens (212) d'extraction de la clé de désembrouillage appliquent une opération prédéterminée à l'information extraite en tant qu'information d'identification de paquet pour générer un identifiant de clé de désembrouillage, et extraient une clé de désembrouillage à partir de la liste sur la base de l'identifiant de la clé de désembrouillage.

10. Dispositif de réception selon la revendication 1, dans lequel les moyens de réception (201) reçoivent séquentiellement un paquet TS incluant (a) l'unité prédéterminée de contenu brouillé et (b) une information d'image I non embrouillée, l'information d'image I indiquant si le paquet de flux TS correspondant à l'information est constitué par une partie d'une image I et/ou d'une image I ou non; et
les moyens de mémoire (202) mémorisent séquentiellement le paquet de flux TS reçu,
dans lequel les moyens de traitement de désembrouillage (204) incluent :

des moyens (210) d'extraction du contenu brouillé pour, lors de l'exécution de processus particulier de reproduction, extraire l'unité prédéterminée de contenu brouillé et l'information d'image I à partir de l'un des paquets de flux TS mémorisés dans les moyens de mémoire;
des moyens (204,S52) d'évaluation d'une image I servant à évaluer si l'unité extraite prédéterminée du contenu brouillé est constituée par une partie d'une image I / une image I ou non, sur la base de l'information d'image I extraite;
des moyens (212) d'extraction de la clé de désembrouillage pour extraire une clé de désembrouillage à partir de la liste uniquement lorsque l'unité extraite prédéterminée du contenu brouillé est constituée par une partie d'une image I / une image I; et
des moyens de désembrouillage (211) pour désembrouiller l'unité extraite prédéterminée du contenu brouillé en utilisant la clé de désembrouillage extraite;

11. Dispositif de réception selon la revendication 1 gérant en outre une information de contrat et constitué par un module de sécurité dont la partie ne fonctionne pas effectivement si un contrat n'a pas été passé, et d'autres modules, le dispositif de réception comprenant en outre:

des moyens (203) de conservation de liste pour conserver la liste extraite par les moyens d'extraction de liste,

dans lequel les moyens (301) d'extraction de liste et les moyens (203) de conservation de liste sont prévus à l'intérieur du module de sécurité.

12. Dispositif de diffusion (100) pour brouiller un contenu et diffuser le contenu brouillé à un dispositif de réception (200), le dispositif de diffusion (100) comprenant :

des moyens d'acquisition (106,107) pour acquérir le contenu devant être brouillé et une pluralité de clés de désembrouillage;
des moyens (103) de traitement de brouillage pour brouiller une unité prédéterminée d'un contenu à partir du contenu acquis de sorte que l'unité prédéterminée du contenu brouillé est désembrouillée en utilisant une clé de désembrouillage différente pour chaque unité prédéterminée ou pour chaque ensemble d'une pluralité d'unités prédéterminée; et
des moyens de diffusion (105) sont agencés de manière à diffuser le contenu brouillé;

caractérisé en ce que :

le dispositif de diffusion (100) comprend en outre :

des moyens (102) de production de liste servant à générer une liste des clés de désembrouillage; et des moyens d'insertion (104) pour insérer la liste dans au moins un élément d'une information prédéterminée pour générer au moins un élément d'information de mémoire, et
les moyens de diffusion (105) sont agencés de manière à diffuser l'information de mémoire générée,

13. Dispositif de diffusion selon la revendication 12, dans lequel des moyens d'insertion (104) insèrent la liste dans un élément d'information prédéterminée pour générer un élément d'information de mémoire, et
les moyens de diffusion (105) diffusent l'élément gé-

néré d'information et le contenu brouillé.

14. Dispositif de diffusion selon la revendication 12, dans lequel
les moyens d'insertion insèrent une partie divisée de la liste dans chacun d'une pluralité d'éléments d'information prédéterminée pour générer une pluralité d'éléments d'information de mémoire, et
les moyens de diffusion (105) diffusent la pluralité générée d'éléments d'information de mémoire et le contenu brouillé.

15. Dispositif de diffusion selon la revendication 12, dans lequel les moyens d'insertion (104) insèrent la liste dans une partie devant être codée dans un corps principal d'au moins un message ECM pour générer au moins un élément d'information de mémoire.

16. Dispositif de diffusion selon la revendication 12, dans lequel
les moyens de diffusion (105) diffusent un ensemble de l'information de mémoire alors que la totalité du contenu brouillé correspond à un ordre désembrouillé.

17. Programme informatique comprenant un code informatique servant, lorsqu'il est chargé dans un système informatique et est exécuté, à amener ledit système informatique à exécuter les étapes suivantes :

une étape de réception (S21) pour recevoir un contenu brouillé, le contenu brouillé étant brouillé de telle sorte qu'une unité prédéterminée du contenu brouillé, qui est une partie du contenu brouillé, est désembrouillé en utilisant une clé de désembrouillage correspondant à une unité prédéterminée de contenu brouillé;
une étape de mémoire (S22) pour mémoriser le contenu brouillé reçu;
une étape de traitement de désembrouillage (S33) pour (a) extraire l'unité prédéterminée du contenu brouillé à partir du contenu brouillé mémorisé, et (b) obtenir une unité prédéterminée de contenu à partir de l'unité prédéterminée extraite du contenu brouillé; et
une étape de reproduction (S34) pour reproduire l'unité prédéterminée du contenu dans l'ordre obtenu,

caractérisé en ce que :

l'étape de réception (S21) sert en outre à recevoir au moins un élément d'information de mémoire, dans lesquels est insérée une liste incluant toutes les clés de désembrouillage devant être utilisées pour désembrouiller le contenu brouillé,
l'étape de mémorisation (S22) sert en outre à mémoriser l'information de mémoire reçue,
le code informatique amène en outre ledit système informatique à exécuter une étape (S31) d'extraction de liste pour extraire la liste à partir de l'information de mémoire mémorisée, et
l'étape de traitement de désembrouillage (S33) sert en outre à extraire une clé de désembrouillage correspondant à l'unité prédéterminée du contenu brouillé à partir de la liste extraite, et à obtenir l'unité prédéterminée de contenu par désembrouillage de l'unité prédéterminée extraite du contenu brouillé moyennant l'utilisation de la clé de désembrouillage extraite.

18. Programme informatique comprenant un code informatique pour, lorsqu'il est chargé dans un système informatique et est exécuté, amener ledit système informatique à exécuter les étapes suivantes :

une étape d'acquisition (S1,S3) pour acquérir un contenu devant être brouillé et une pluralité de clés de désembrouillage;
une étape de traitement de brouillage (S5) pour brouiller une unité prédéterminée du contenu à partir du contenu acquis de sorte que l'unité prédéterminée du contenu brouillé est désembrouillée moyennant l'utilisation d'une clé de désembrouillage différente pour chaque unité prédéterminée ou chaque ensemble d'une pluralité d'unités prédéterminées; et
une étape de diffusion (S7) pour diffuser le contenu brouillé,

caractérisé en ce que :

le code informatique amène en outre ledit système informatique à exécuter : une étape (S4) de production de liste pour générer une liste des clés de désembrouillage; et une étape d'insertion (S6) pour insérer la liste dans au moins un élément d'information prédéterminée pour générer au moins un élément d'information de mémoire, et
l'étape de diffusion (S7) et sert en outre à diffuser l'information de mémoire générée.

19. Support d'enregistrement pour mémoriser des informations qui amènent au moins une partie d'un système informatique à suivre les étapes suivantes :

une étape de réception (S21) pour recevoir un contenu brouillé, le contenu brouillé étant brouillé de telle sorte qu'une unité prédéterminée du contenu brouillé, qui est une partie du contenu brouillé, est désembrouillée moyennant l'utilisation d'une clé de désembrouillage correspondant à l'unité prédéterminée de contenu brouillé,

une étape de mémoire (S22) pour mémoriser le contenu brouillé reçu;
une étape de traitement de désembrouillage (S33) pour (a) extraire l'unité prédéterminée de contenu brouillé à partir du contenu brouillé mémorisé, et (b) obtenir une unité prédéterminée de contenu à partir de l'unité prédéterminée extraite du contenu brouillé; et
une étape de reproduction (S34) pour reproduire l'unité prédéterminée de contenu dans l'ordre obtenu,

caractérisé en ce que :

l'étape de réception (S21) sert en outre à recevoir au moins un élément d'information de mémoire, dans lequel est insérée une liste incluant tous les codes de désembrouillage devant être utilisé pour désembrouiller le contenu brouillé,
l'étape de mémoire (S22) sert en outre à mémoriser l'information de mémoire reçue; et
les instructions amènent en outre ledit système informatique à exécuter une étape (S31) d'extraction de liste pour extraire la liste à partir de l'information de mémoire mémorisée;

20. Support d'enregistrement pour mémoriser des instructions qui amènent au moins une partie d'un système informatique pour exécuter les étapes suivantes:

une étape d'acquisition (S1,S3) pour acquérir le contenu devant être brouillé et une pluralité de clés de désembrouillage;
une étape de traitement de brouillage (S5) pour brouiller une unité prédéterminée du contenu à partir du contenu acquis de sorte que l'unité prédéterminée du contenu brouillé est désembrouillée en utilisant une clé de désembrouillage différente pour chaque unité prédéterminée ou chaque ensemble d'une pluralité d'unités prédéterminées; et
une étape de diffusion (S7) pour diffuser le contenu brouillé,

caractérisé en ce que:

des instructions amènent en outre ledit système informatique à exécuter : une étape (S4) de production de liste pour générer une liste des clés de désembrouillage; et une étape d'insertion (S6) pour insérer la liste dans au moins un élément d'information prédéterminée pour générer au moins un élément d'information de mémoire, et
l'étape de diffusion (S7) sert en outre à diffuser l'information de mémoire générée.

21. Procédé de réception et de reproduction d'un contenu brouillé, le procédé comprenant les étapes comprenant :

une étape de réception (S21) pour recevoir le contenu brouillé, le contenu brouillé étant brouillé de telle sorte qu'une unité prédéterminée du contenu brouillé, qui est une partie du contenu brouillé, est désembrouillé moyennant l'utilisation d'une clé de désembrouillage correspondant à l'unité prédéterminée du contenu brouillé;
une étape de mémoire (S22) pour mémoriser le contenu brouillé reçu;
une étape de traitement de désembrouillage (S33) pour (a) extraire l'unité prédéterminée du contenu brouillé à partir du contenu brouillé mémorisé et (b) obtenir une unité prédéterminée de contenu à partir de l'unité prédéterminée extraite et du contenu brouillé; et
une étape de reproduction (S34) pour reproduire l'unité prédéterminée de contenu dans l'ordre obtenu,

caractérisé en ce que l'étape de réception (S21) sert en outre à recevoir au moins un élément d'information de mémoire, dans lequel est insérée une liste incluant toutes les clés de désembrouillage devant être utilisées pour désembrouiller le contenu brouillé,
l'étape de mémorisation (S22) sert en outre à mémoriser l'information de mémoire reçue, et
le procédé comprend en outre une étape d'extraction de liste (S31) pour extraire la liste à partir de l'information de mémoire mémorisée.

22. Procédé pour brouiller un contenu et diffuser le contenu brouillé vers un appareil de réception (200), le procédé comprenant les étapes comprenant :

une étape d'acquisition (S1,S3) pour acquérir le contenu devant être brouillé et une pluralité de clés de désembrouillage;
une étape de traitement de brouillage (SS) pour le brouillage d'une unité prédéterminée du contenu à partir du contenu acquis de sorte que l'unité prédéterminée du contenu brouillé est désembrouillée en utilisant une clé de désembrouillage différente pour chaque unité prédéterminée ou chaque ensemble d'une pluralité d'unités prédéterminée; et
une étape de diffusion (S7) pour la diffusion du contenu brouillé,

caractérisé en ce que :

le procédé comprend en outre : une étape (S4) de production de liste pour produire une liste

des clés de désembrouillage; et une étape d'insertion (S6) pour insérer la liste dans au moins un élément d'information prédéterminé pour générer au moins un élément d'information de mémoire, et
l'étape de diffusion (S7) sert en outre à diffuser l'information de mémoire générée.

FIG. 1

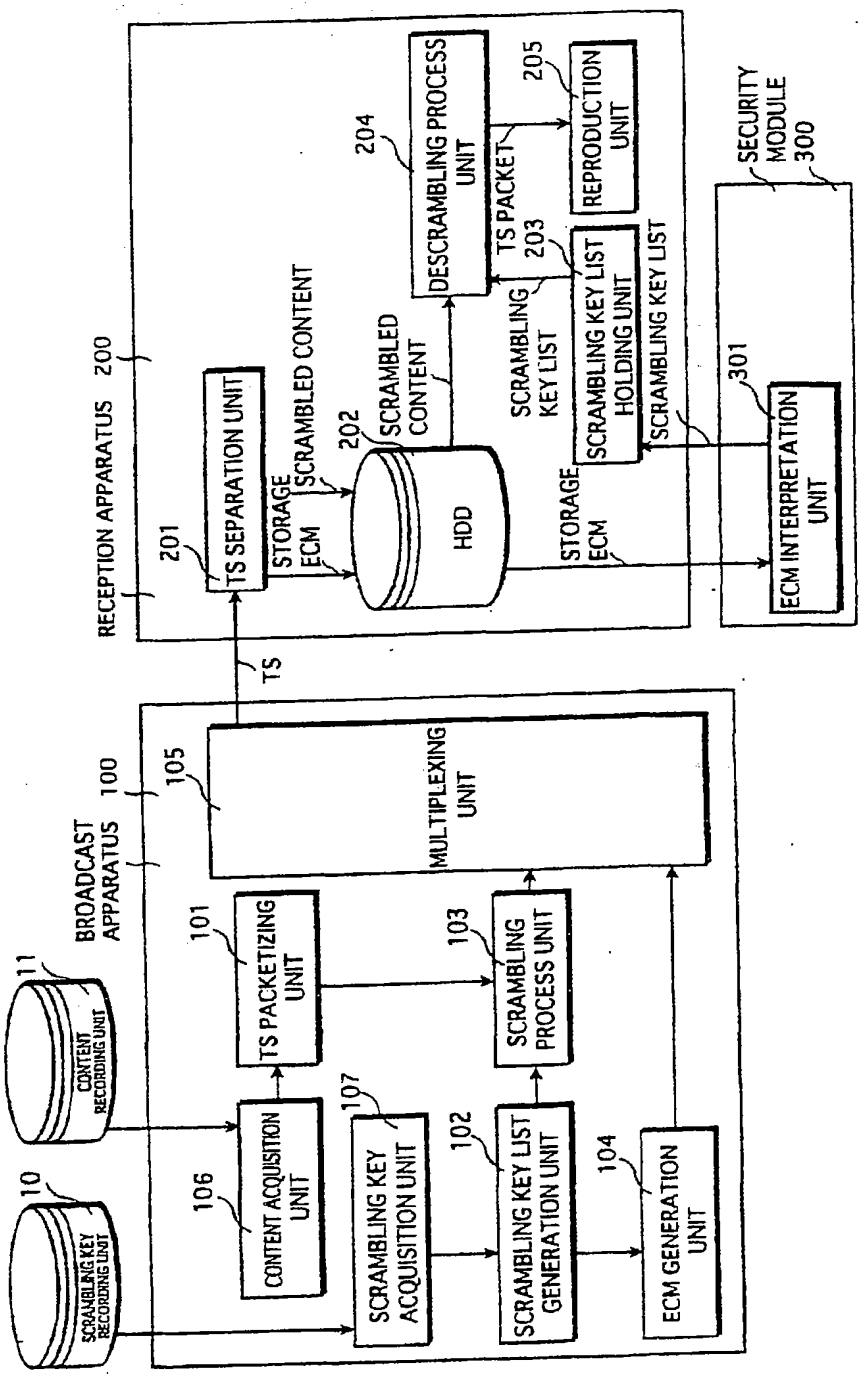

BROADCAST APPARATUS 100
SCRAMBLING KEY RECORDING UNIT 10
CONTENT RECORDING UNIT 11
CONTENT ACQUISITION UNIT 106
SCRAMBLING KEY ACQUISITION UNIT 107
TS PACKETIZING UNIT 101
SCRAMBLING KEY LIST GENERATION UNIT 102
SCRAMBLING PROCESS UNIT 103
ECM GENERATION UNIT 104
MULTIPLEXING UNIT 105
TS
RECEPTION APPARATUS 200
TS SEPARATION UNIT 201
STORAGE
ECM
SCRAMBLED CONTENT
HDD 202
SCRAMBLED CONTENT
SCRAMBLING KEY LIST
SCRAMBLING KEY LIST HOLDING UNIT 203
DESCRAMBLING PROCESS UNIT 204
TS PACKET
REPRODUCTION UNIT 205
STORAGE
ECM
SCRAMBLING KEY LIST
SECURITY MODULE 300
ECM INTERPRETATION UNIT 301

FIG.2

DATA STRUCTURE OF SCRAMBLING KEY LIST DESCRIPTOR

CA_Ks_List_descriptor() {	
descriptor_tag	1 BYTE
descriptor_length	1 BYTE
for(i=0; i <N; i++) {	
Ks_id	1 BYTE
TS_packet_number	2 BYTES
Ks	8 BYTES
}	
}	

Ks_id	:SCRAMBLING KEY IDENTIFIER (TO IDENTIFY SCRAMBLING KEYS)
TS_packet_number	:THE NUMBER OF TS PACKETS SCRAMBLED WITH THE Ks
Ks	:SCRAMBLING KEY

FIG.3

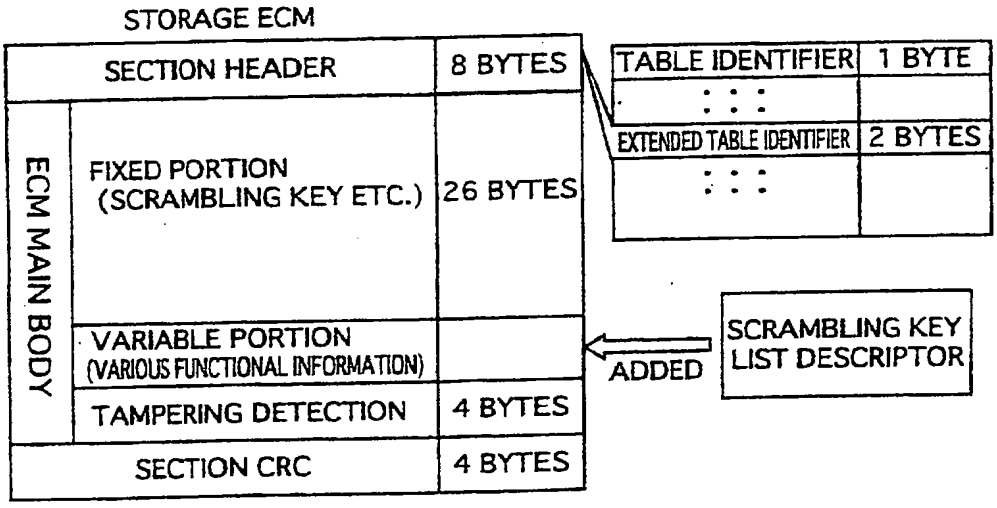

STORAGE ECM
SECTION HEADER
8 BYTES
ECM MAIN BODY
FIXED PORTION (SCRAMBLING KEY ETC.)
26 BYTES
VARIABLE PORTION (VARIOUS FUNCTIONAL INFORMATION)
TAMPERING DETECTION
4 BYTES
SECTION CRC
4 BYTES
TABLE IDENTIFIER
1 BYTE
EXTENDED TABLE IDENTIFIER
2 BYTES
ADDED
SCRAMBLING KEY LIST DESCRIPTOR

FIG.4

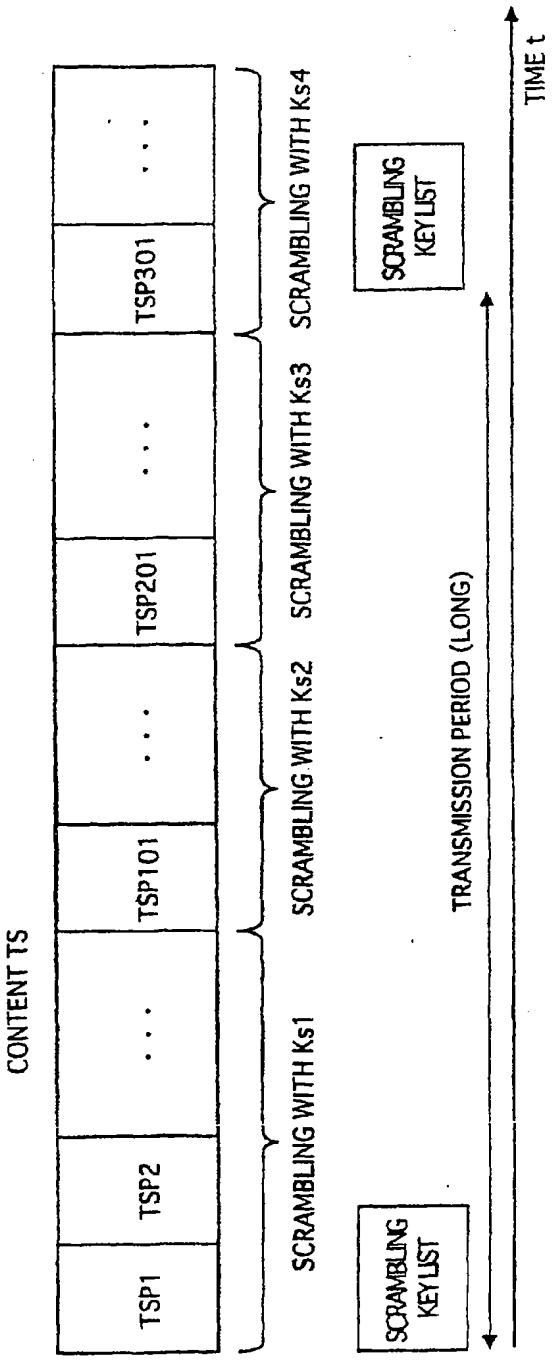

CONTENT TS
TSP1
TSP2
TSP101
TSP201
TSP301
SCRAMBLING WITH Ks1
SCRAMBLING WITH Ks2
SCRAMBLING WITH Ks3
SCRAMBLING WITH Ks4
SCRAMBLING KEY LIST
SCRAMBLING KEY LIST
TRANSMISSION PERIOD (LONG)
TIME t
TSP :TS PACKET
Ks :SCRAMBLING KEY

FIG.5

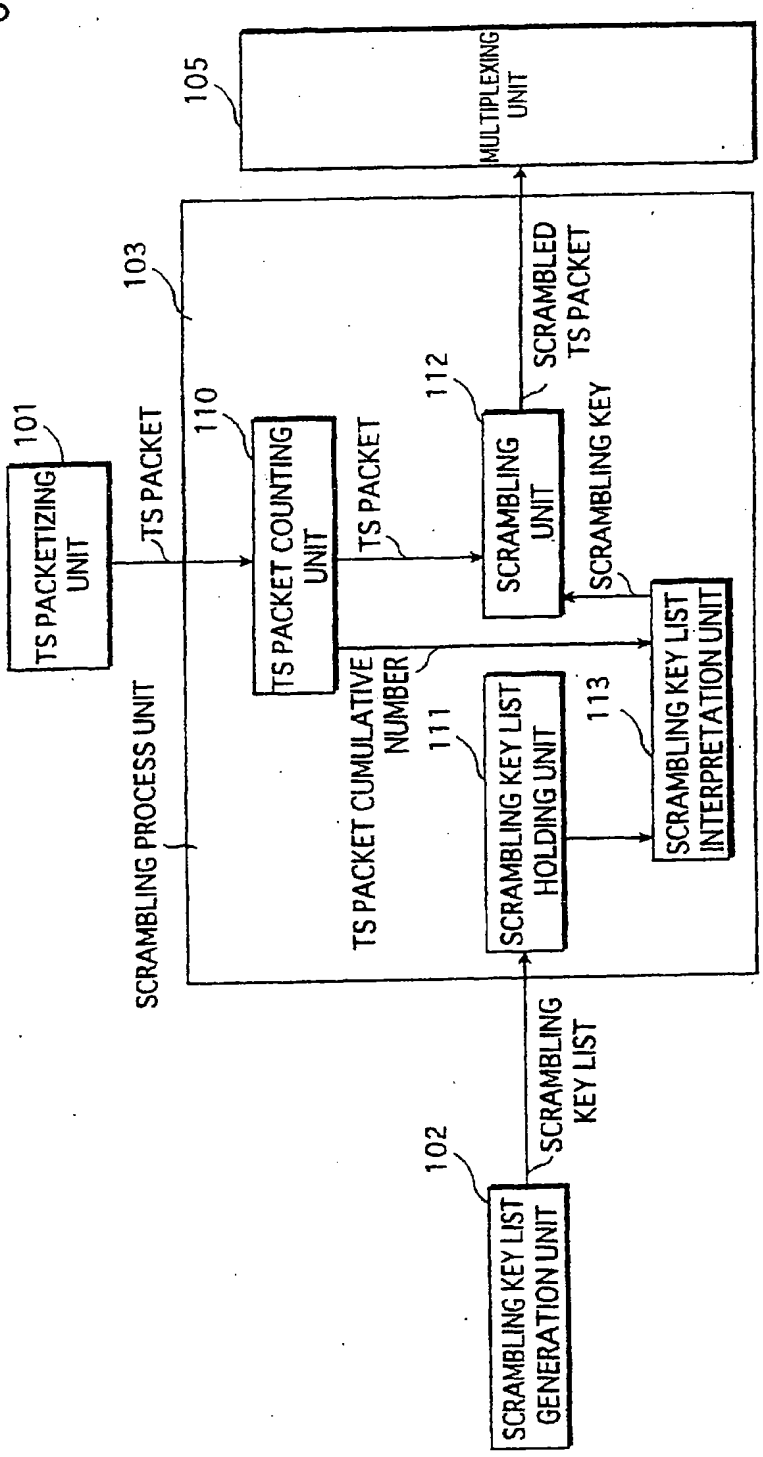

105
MULTIPLEXING UNIT
103
SCRAMBLING PROCESS UNIT
101
TS PACKETIZING UNIT
TS PACKET
110
TS PACKET COUNTING UNIT
TS PACKET
112
SCRAMBLING UNIT
SCRAMBLED TS PACKET
SCRAMBLING KEY
TS PACKET CUMULATIVE NUMBER
111
SCRAMBLING KEY LIST HOLDING UNIT
113
SCRAMBLING KEY LIST INTERPRETATION UNIT
SCRAMBLING KEY LIST
102
SCRAMBLING KEY LIST GENERATION UNIT

FIG.6

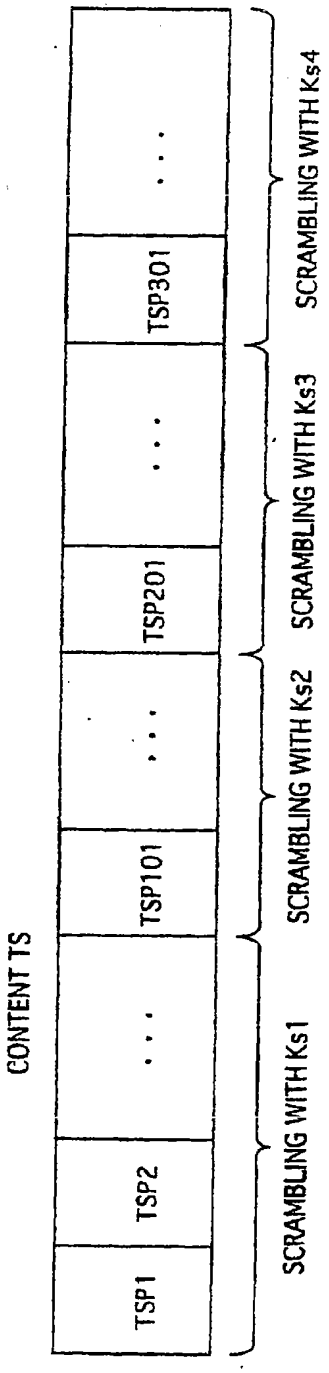

CONTENT TS
TSP1
TSP2
TSP101
TSP201
TSP301
SCRAMBLING WITH Ks1
SCRAMBLING WITH Ks2
SCRAMBLING WITH Ks3
SCRAMBLING WITH Ks4
TSP :TS PACKET
Ks :SCRAMBLING KEY

FIG.7

SCRAMBLING KEY LIST

Ks_id TS_packet_number Ks	1 100 Ks 1
Ks_id TS_packet_number Ks	2 100 Ks 2
Ks_id TS_packet_number Ks	3 100 Ks 3
Ks_id TS_packet_number Ks	4 100 Ks 4

FIG.8

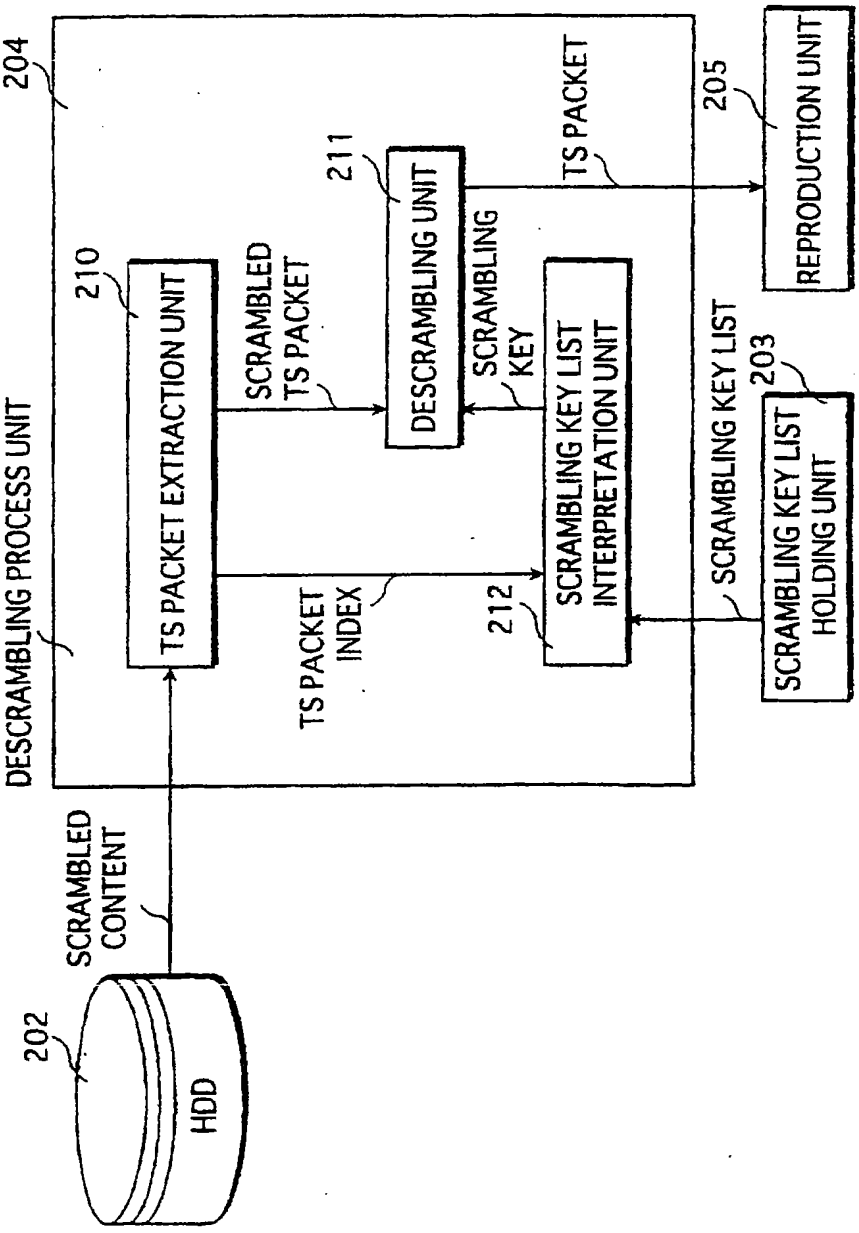

DESCRAMBLING PROCESS UNIT
204
TS PACKET EXTRACTION UNIT
210
DESCRAMBLING UNIT
211
SCRAMBLING KEY LIST INTERPRETATION UNIT
212
SCRAMBLING KEY LIST HOLDING UNIT
203
REPRODUCTION UNIT
205
SCRAMBLED TS PACKET
SCRAMBLING KEY
TS PACKET
TS PACKET INDEX
SCRAMBLING KEY LIST
SCRAMBLED CONTENT
HDD
202

FIG.9

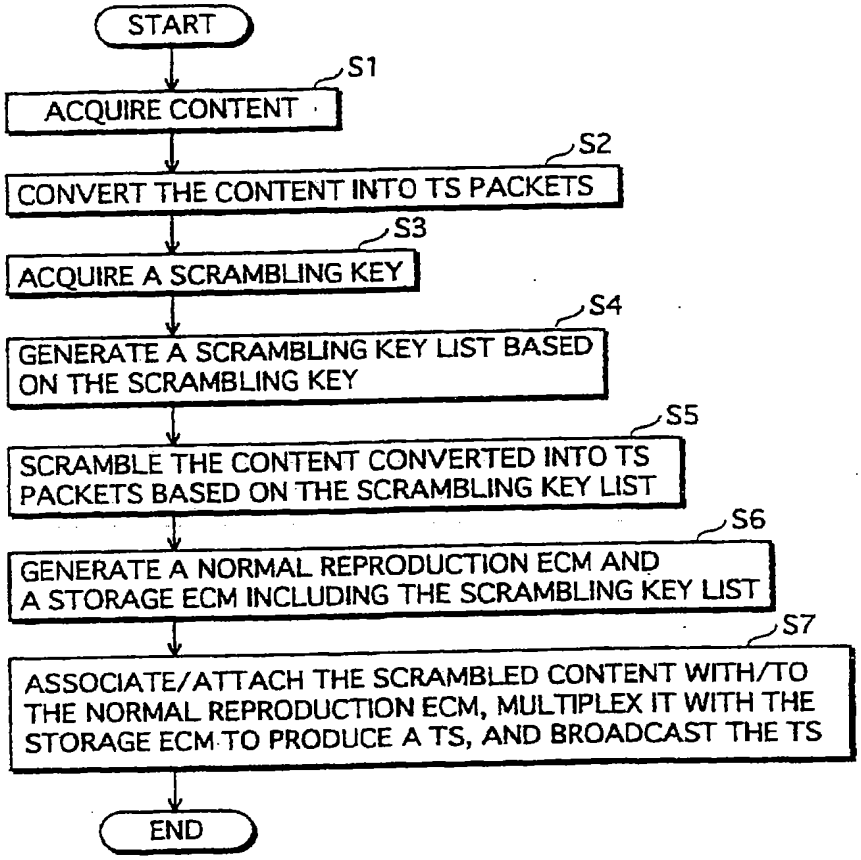

START
S1
ACQUIRE CONTENT
S2
CONVERT THE CONTENT INTO TS PACKETS
S3
ACQUIRE A SCRAMBLING KEY
S4
GENERATE A SCRAMBLING KEY LIST BASED ON THE SCRAMBLING KEY
S5
SCRAMBLE THE CONTENT CONVERTED INTO TS PACKETS BASED ON THE SCRAMBLING KEY LIST
S6
GENERATE A NORMAL REPRODUCTION ECM AND A STORAGE ECM INCLUDING THE SCRAMBLING KEY LIST
S7
ASSOCIATE/ATTACH THE SCRAMBLED CONTENT WITH/TO THE NORMAL REPRODUCTION ECM, MULTIPLEX IT WITH THE STORAGE ECM TO PRODUCE A TS, AND BROADCAST THE TS
END

FIG.10

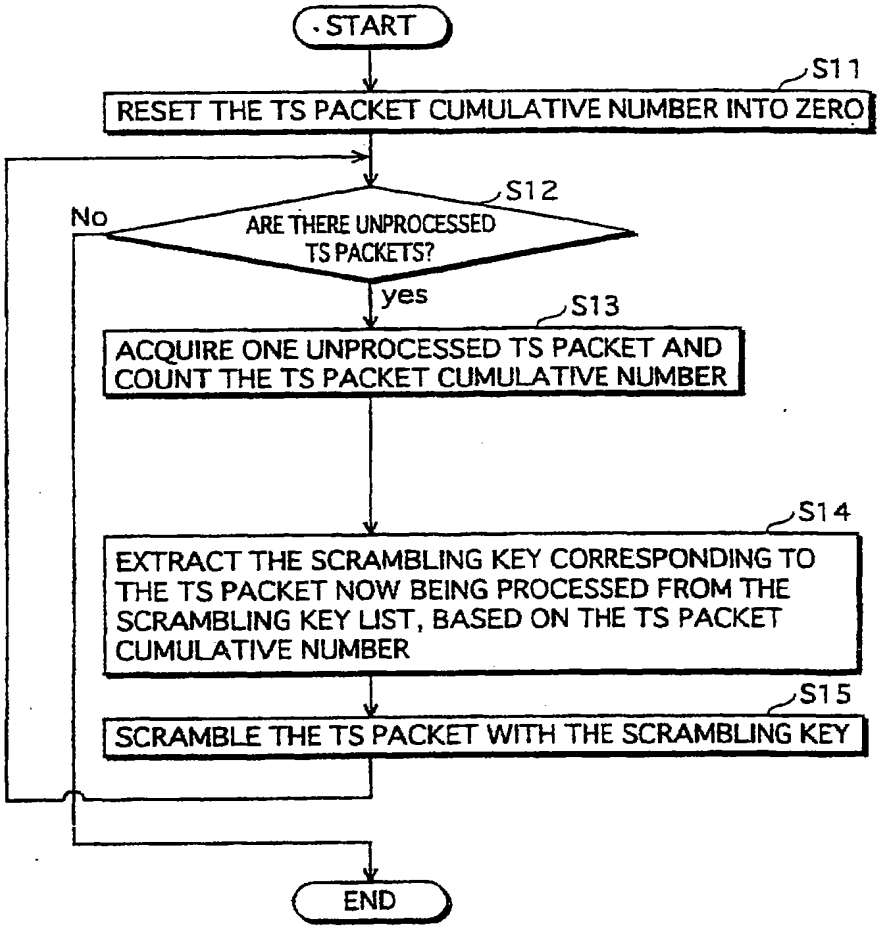

START
S11
RESET THE TS PACKET CUMULATIVE NUMBER INTO ZERO
S12
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S13
ACQUIRE ONE UNPROCESSED TS PACKET AND COUNT THE TS PACKET CUMULATIVE NUMBER
S14
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE TS PACKET NOW BEING PROCESSED FROM THE SCRAMBLING KEY LIST, BASED ON THE TS PACKET CUMULATIVE NUMBER
S15
SCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG. 11

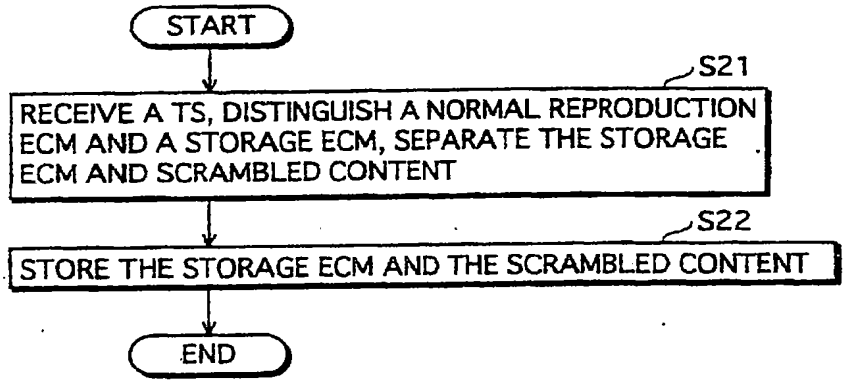

START
S21
RECEIVE A TS, DISTINGUISH A NORMAL REPRODUCTION ECM AND A STORAGE ECM, SEPARATE THE STORAGE ECM AND SCRAMBLED CONTENT
S22
STORE THE STORAGE ECM AND THE SCRAMBLED CONTENT
END

FIG.12

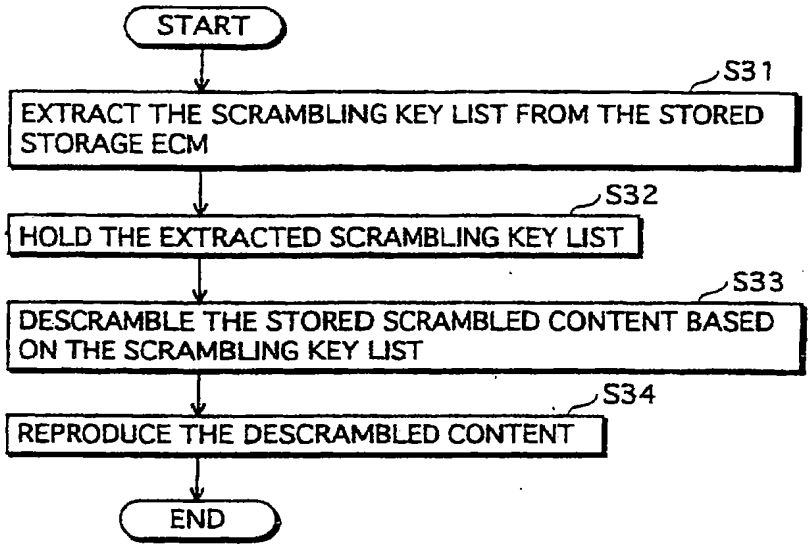

START
S31
EXTRACT THE SCRAMBLING KEY LIST FROM THE STORED STORAGE ECM
S32
HOLD THE EXTRACTED SCRAMBLING KEY LIST
S33
DESCRAMBLE THE STORED SCRAMBLED CONTENT BASED ON THE SCRAMBLING KEY LIST
S34
REPRODUCE THE DESCRAMBLED CONTENT
END

FIG.13

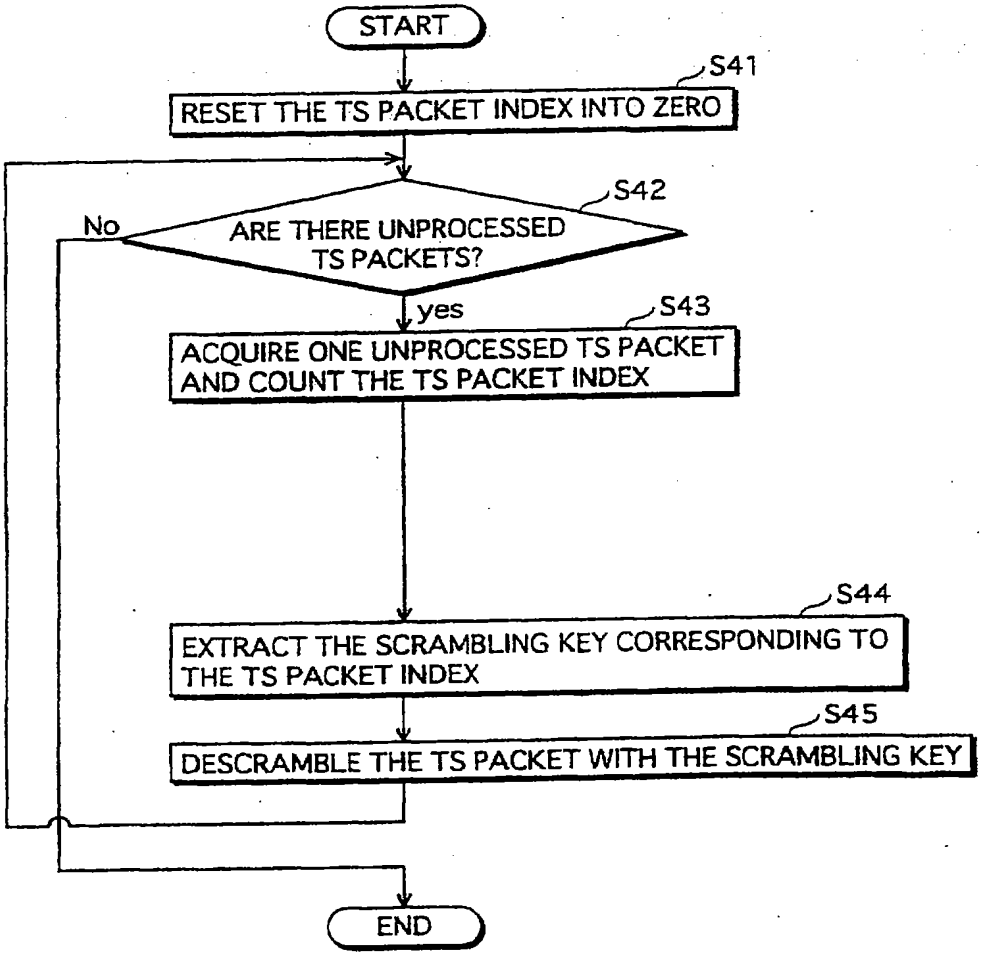

START
S41
RESET THE TS PACKET INDEX INTO ZERO
S42
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S43
ACQUIRE ONE UNPROCESSED TS PACKET AND COUNT THE TS PACKET INDEX
S44
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE TS PACKET INDEX
S45
DESCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG.14

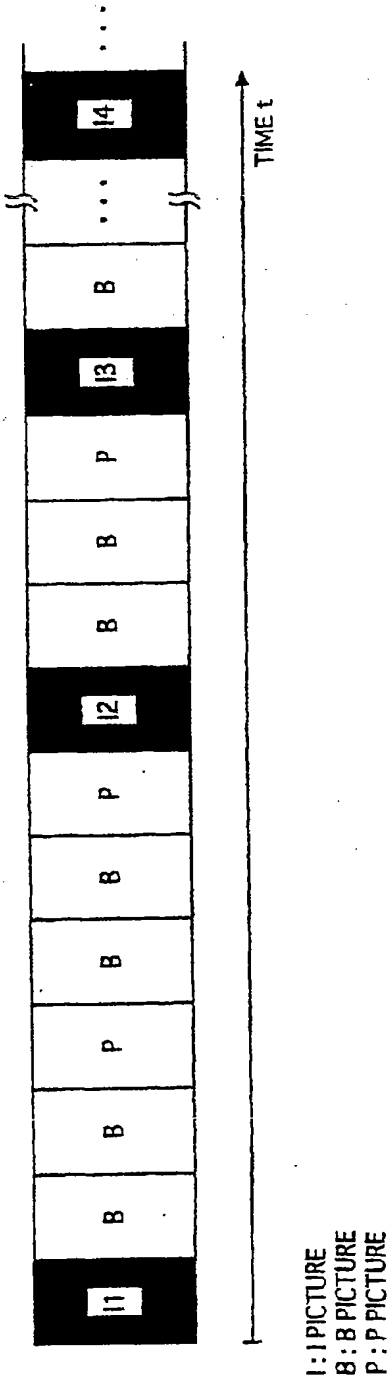

I1
B
B
P
B
B
P
B
B
I2
B
B
P
B
B
I3
B
...
I4
...
TIME t
I : I PICTURE
B : B PICTURE
P : P PICTURE

FIG.15

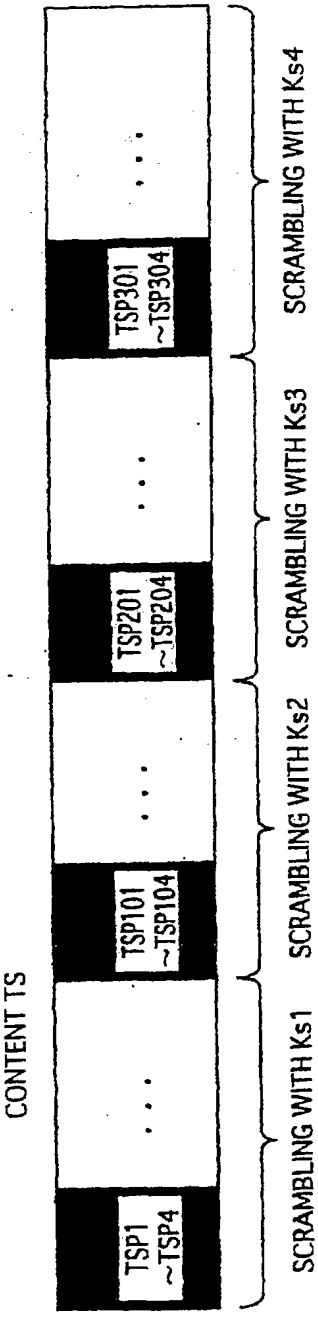

CONTENT TS
TSP1 ~TSP4
TSP101 ~TSP104
TSP201 ~TSP204
TSP301 ~TSP304
SCRAMBLING WITH Ks1
SCRAMBLING WITH Ks2
SCRAMBLING WITH Ks3
SCRAMBLING WITH Ks4
TSP :TS PACKET
Ks :SCRAMBLING KEY

FIG.16

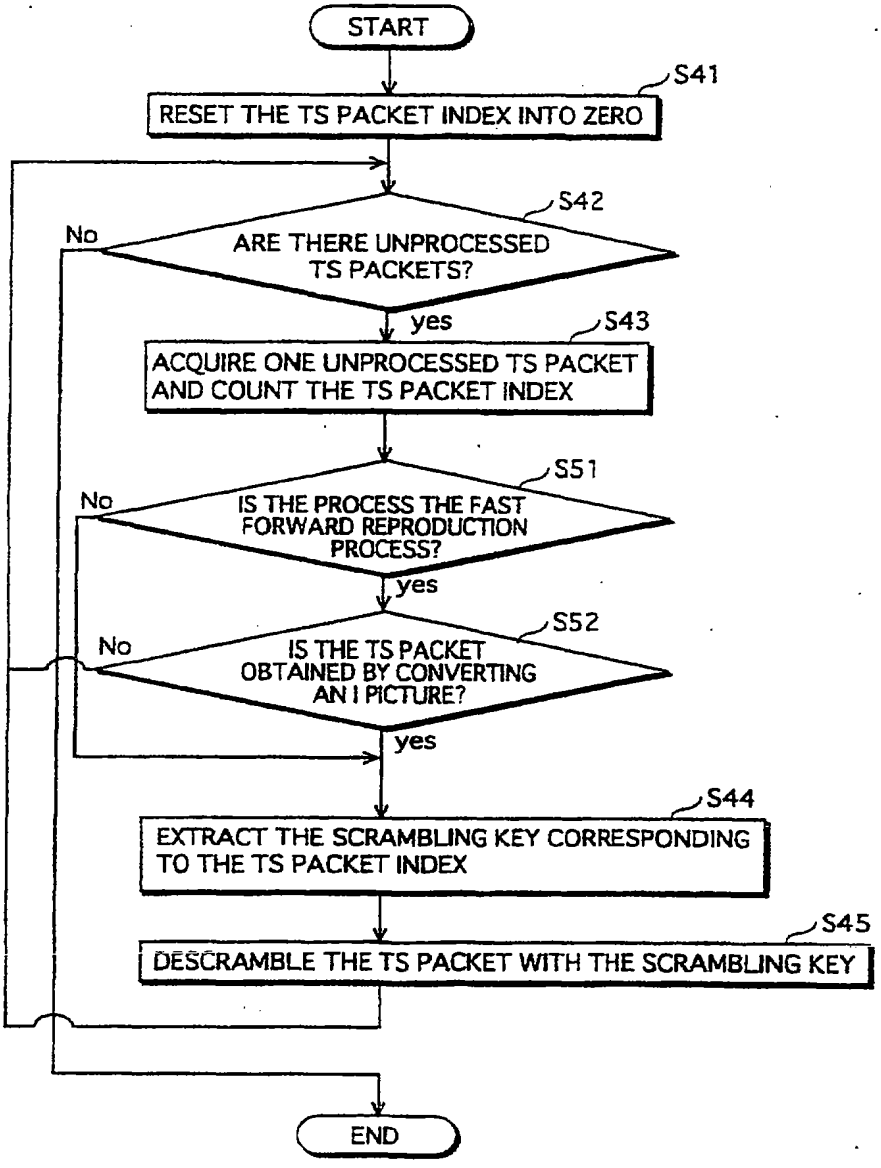

START
S41
RESET THE TS PACKET INDEX INTO ZERO
S42
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S43
ACQUIRE ONE UNPROCESSED TS PACKET AND COUNT THE TS PACKET INDEX
S51
No
IS THE PROCESS THE FAST FORWARD REPRODUCTION PROCESS?
yes
S52
No
IS THE TS PACKET OBTAINED BY CONVERTING AN I PICTURE?
yes
S44
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE TS PACKET INDEX
S45
DESCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG.17

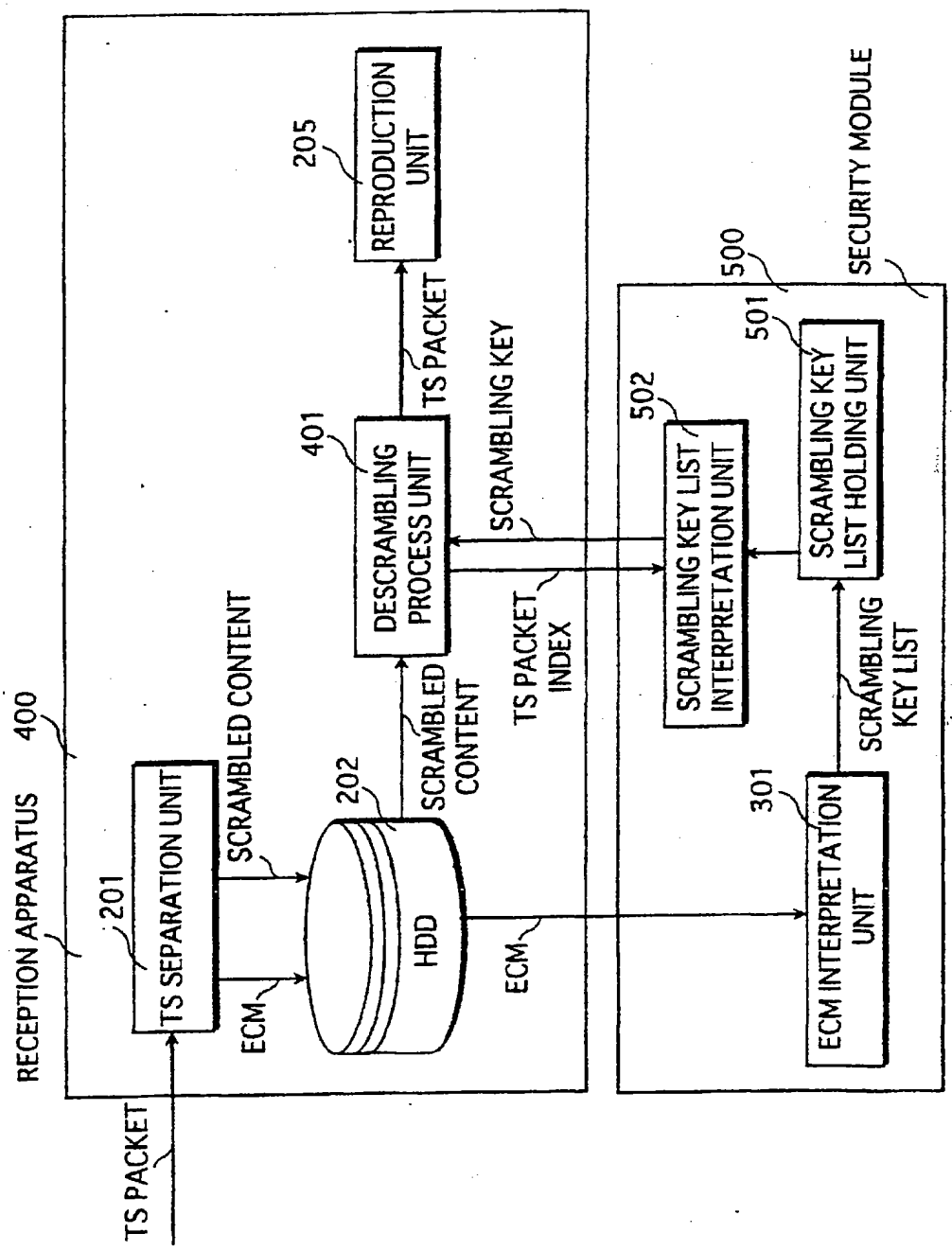

RECEPTION APPARATUS
400
TS PACKET
TS SEPARATION UNIT
201
SCRAMBLED CONTENT
ECM
HDD
202
SCRAMBLED CONTENT
DESCRAMBLING PROCESS UNIT
401
REPRODUCTION UNIT
205
TS PACKET
SCRAMBLING KEY
TS PACKET INDEX
ECM
SECURITY MODULE
500
ECM INTERPRETATION UNIT
301
SCRAMBLING KEY LIST
SCRAMBLING KEY LIST INTERPRETATION UNIT
502
SCRAMBLING KEY LIST HOLDING UNIT
501

FIG.18

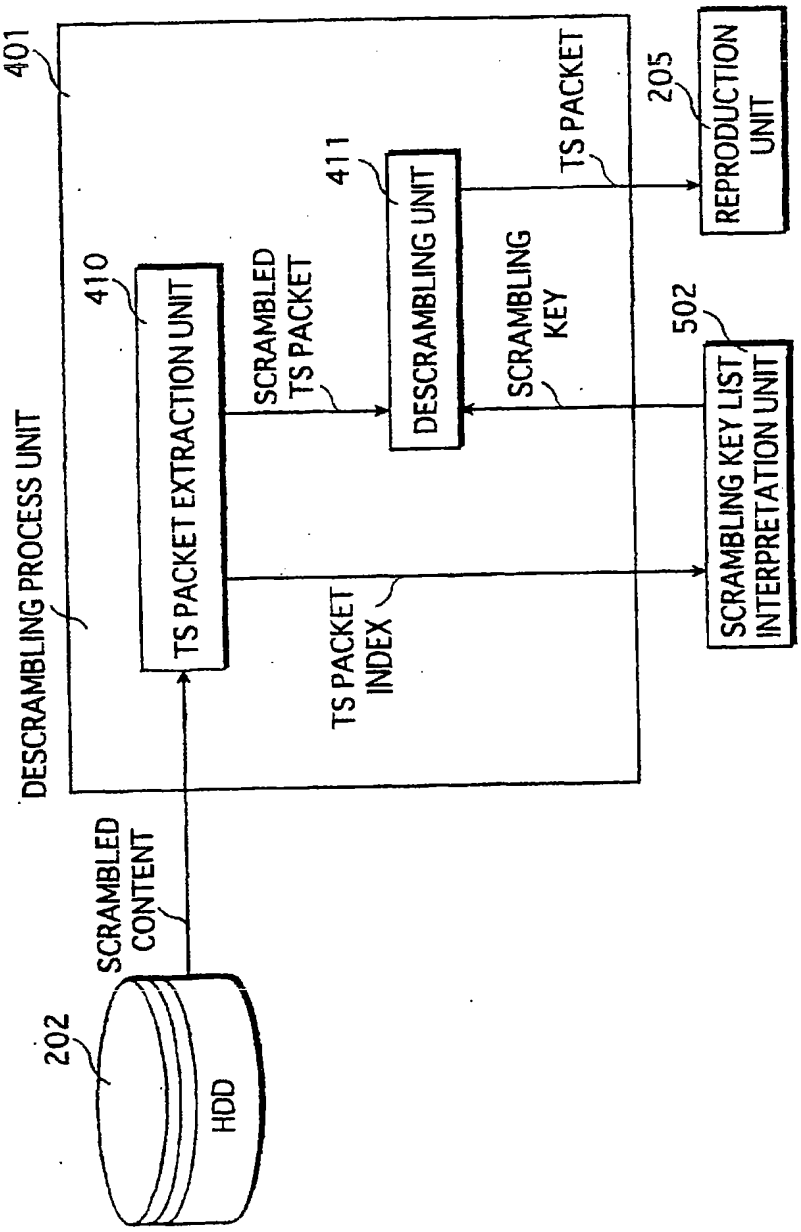

401
DESCRAMBLING PROCESS UNIT
410
TS PACKET EXTRACTION UNIT
SCRAMBLED TS PACKET
411
DESCRAMBLING UNIT
TS PACKET
205
REPRODUCTION UNIT
SCRAMBLING KEY
502
SCRAMBLING KEY LIST INTERPRETATION UNIT
TS PACKET INDEX
SCRAMBLED CONTENT
202
HDD

FIG.19

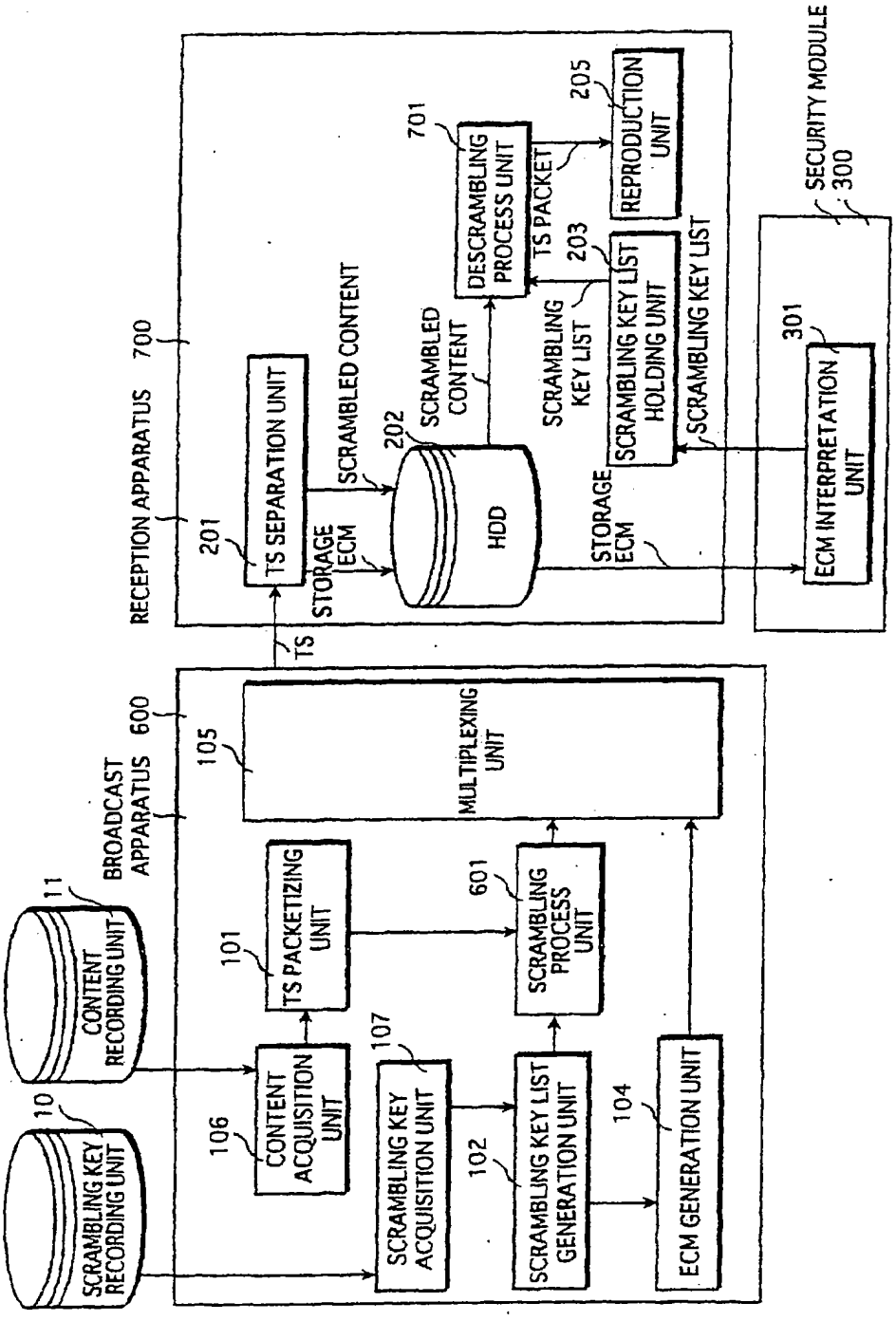

SCRAMBLING KEY RECORDING UNIT
10
CONTENT RECORDING UNIT
11
BROADCAST APPARATUS
600
CONTENT ACQUISITION UNIT
106
TS PACKETIZING UNIT
101
SCRAMBLING KEY ACQUISITION UNIT
107
SCRAMBLING KEY LIST GENERATION UNIT
102
ECM GENERATION UNIT
104
SCRAMBLING PROCESS UNIT
601
MULTIPLEXING UNIT
105
TS
RECEPTION APPARATUS
700
TS SEPARATION UNIT
201
STORAGE ECM
SCRAMBLED CONTENT
HDD
202
SCRAMBLED CONTENT
SCRAMBLING KEY LIST
DESCRAMBLING PROCESS UNIT
701
TS PACKET
REPRODUCTION UNIT
205
SCRAMBLING KEY LIST HOLDING UNIT
203
SCRAMBLING KEY LIST
STORAGE ECM
SECURITY MODULE
300
ECM INTERPRETATION UNIT
301

FIG.20

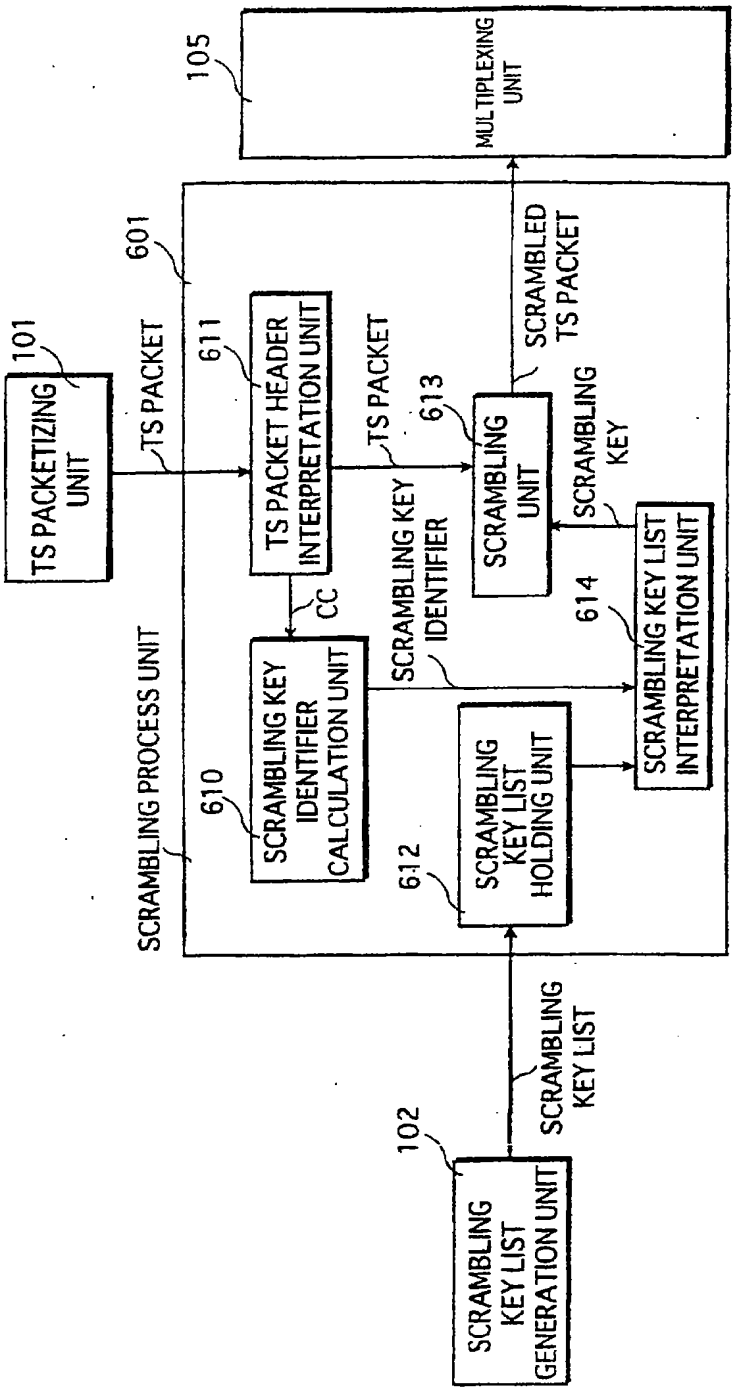

105
MULTIPLEXING UNIT
601
SCRAMBLING PROCESS UNIT
101
TS PACKETIZING UNIT
TS PACKET
611
TS PACKET HEADER INTERPRETATION UNIT
TS PACKET
613
SCRAMBLING UNIT
SCRAMBLED TS PACKET
SCRAMBLING KEY
614
SCRAMBLING KEY LIST INTERPRETATION UNIT
CC
SCRAMBLING KEY IDENTIFIER
610
SCRAMBLING KEY IDENTIFIER CALCULATION UNIT
612
SCRAMBLING KEY LIST HOLDING UNIT
SCRAMBLING KEY LIST
102
SCRAMBLING KEY LIST GENERATION UNIT

FIG.21

SCRAMBLING KEY LIST

Ks_id Ks	0 Ks 1
Ks_id Ks	1 Ks 2
Ks_id Ks	2 Ks 3
Ks_id Ks	3 Ks 4
Ks_id Ks	4 Ks 5
Ks_id Ks	5 Ks 6
Ks_id Ks	6 Ks 7
Ks_id Ks	7 Ks 8
Ks_id Ks	8 Ks 9
Ks_id Ks	9 Ks 10
Ks_id Ks	10 Ks 11
Ks_id Ks	11 Ks 12
Ks_id Ks	12 Ks 13
Ks_id Ks	13 Ks 14
Ks_id Ks	14 Ks 15
Ks_id Ks	15 Ks 16

FIG.22

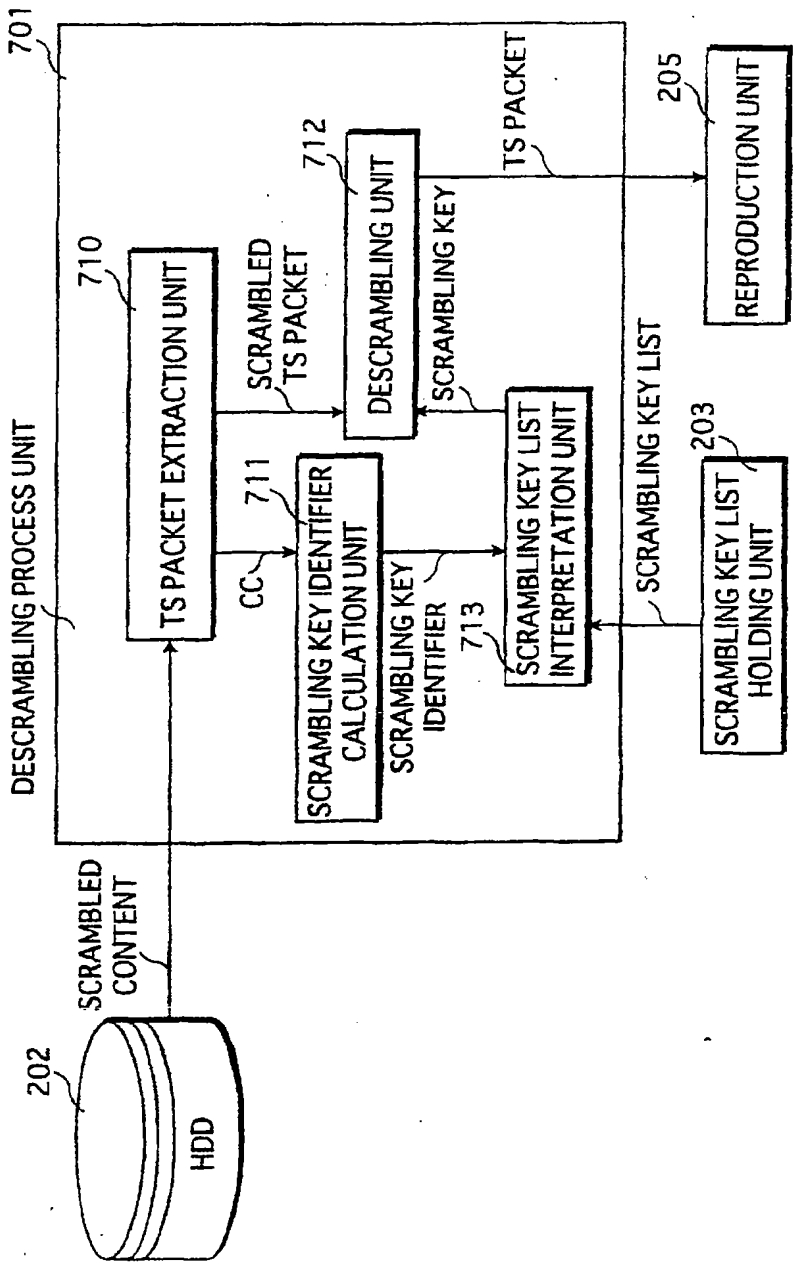

701
DESCRAMBLING PROCESS UNIT
710
TS PACKET EXTRACTION UNIT
711
SCRAMBLING KEY IDENTIFIER CALCULATION UNIT
712
DESCRAMBLING UNIT
713
SCRAMBLING KEY IDENTIFIER
SCRAMBLED TS PACKET
SCRAMBLING KEY
CC
TS PACKET
SCRAMBLING KEY LIST INTERPRETATION UNIT
SCRAMBLING KEY LIST
203
SCRAMBLING KEY LIST HOLDING UNIT
205
REPRODUCTION UNIT
SCRAMBLED CONTENT
202
HDD

FIG.23

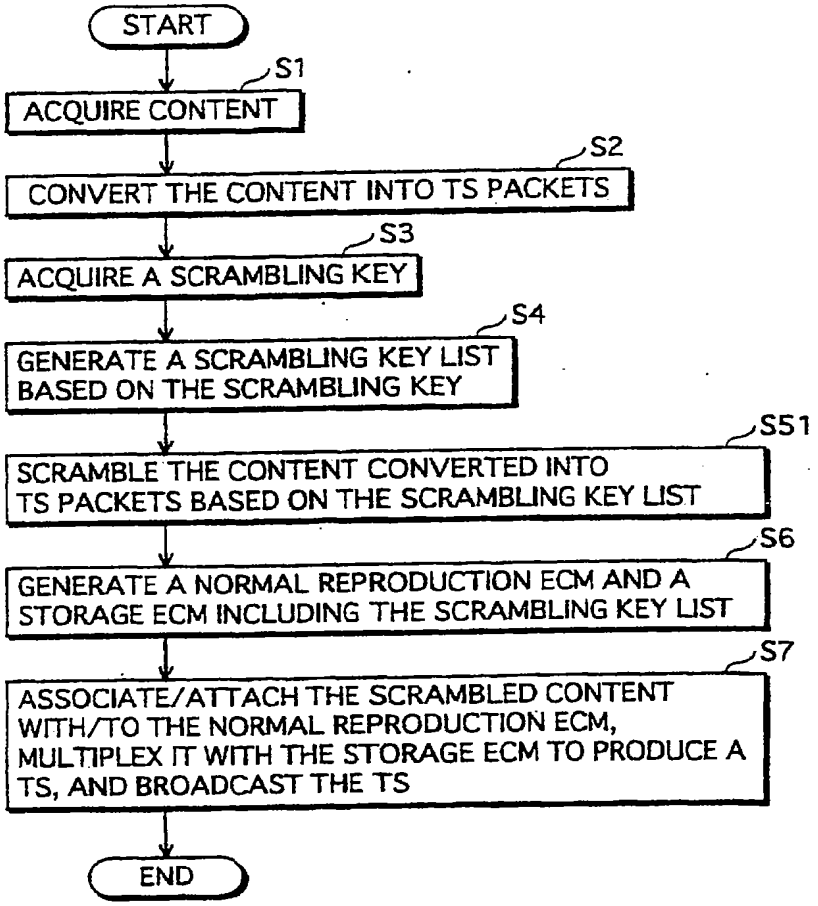

START
S1
ACQUIRE CONTENT
S2
CONVERT THE CONTENT INTO TS PACKETS
S3
ACQUIRE A SCRAMBLING KEY
S4
GENERATE A SCRAMBLING KEY LIST BASED ON THE SCRAMBLING KEY
S51
SCRAMBLE THE CONTENT CONVERTED INTO TS PACKETS BASED ON THE SCRAMBLING KEY LIST
S6
GENERATE A NORMAL REPRODUCTION ECM AND A STORAGE ECM INCLUDING THE SCRAMBLING KEY LIST
S7
ASSOCIATE/ATTACH THE SCRAMBLED CONTENT WITH/TO THE NORMAL REPRODUCTION ECM, MULTIPLEX IT WITH THE STORAGE ECM TO PRODUCE A TS, AND BROADCAST THE TS
END

FIG.24

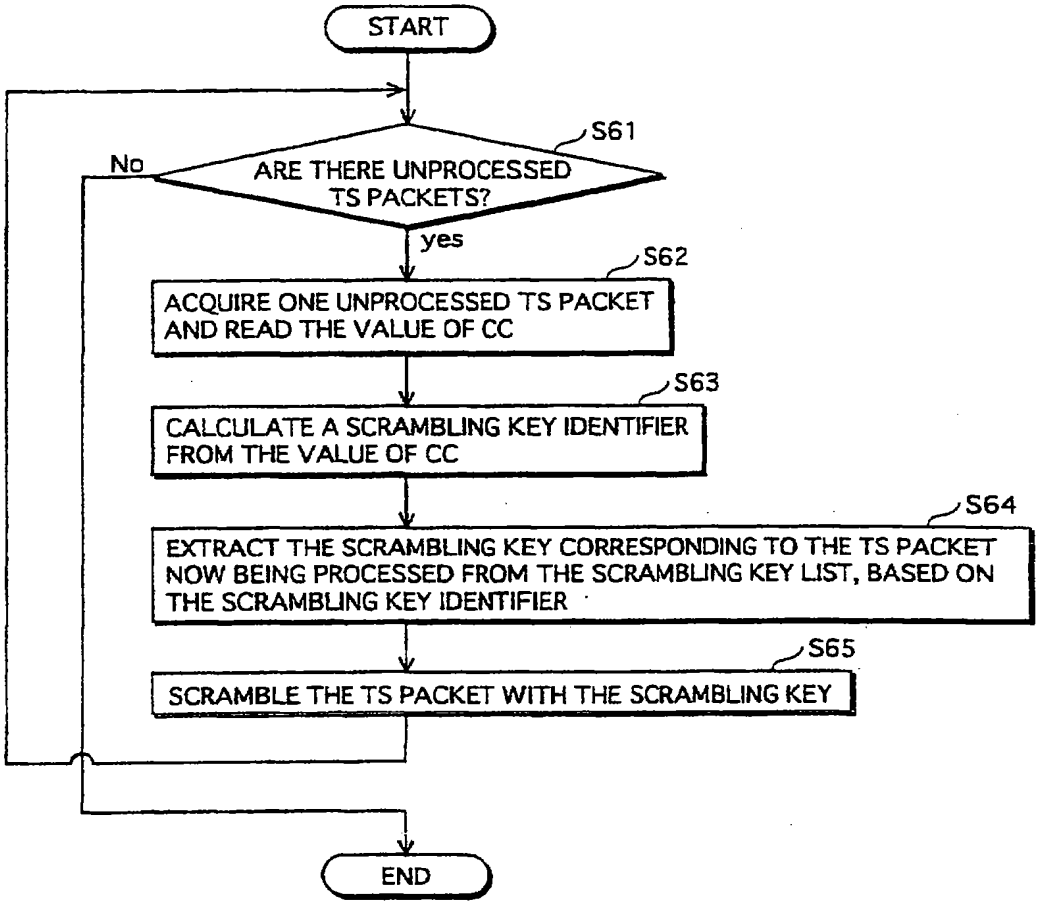

START
S61
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S62
ACQUIRE ONE UNPROCESSED TS PACKET AND READ THE VALUE OF CC
S63
CALCULATE A SCRAMBLING KEY IDENTIFIER FROM THE VALUE OF CC
S64
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE TS PACKET NOW BEING PROCESSED FROM THE SCRAMBLING KEY LIST, BASED ON THE SCRAMBLING KEY IDENTIFIER
S65
SCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG.25

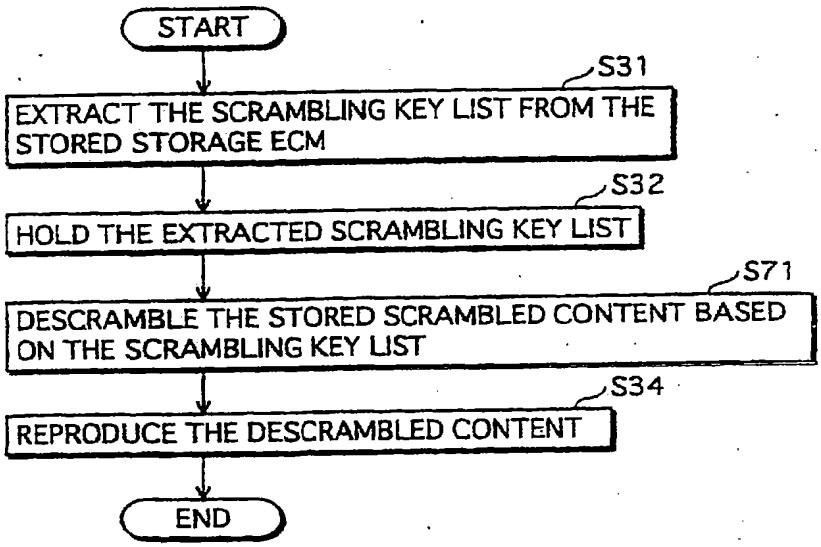

START
S31
EXTRACT THE SCRAMBLING KEY LIST FROM THE STORED STORAGE ECM
S32
HOLD THE EXTRACTED SCRAMBLING KEY LIST
S71
DESCRAMBLE THE STORED SCRAMBLED CONTENT BASED ON THE SCRAMBLING KEY LIST
S34
REPRODUCE THE DESCRAMBLED CONTENT
END

FIG.26

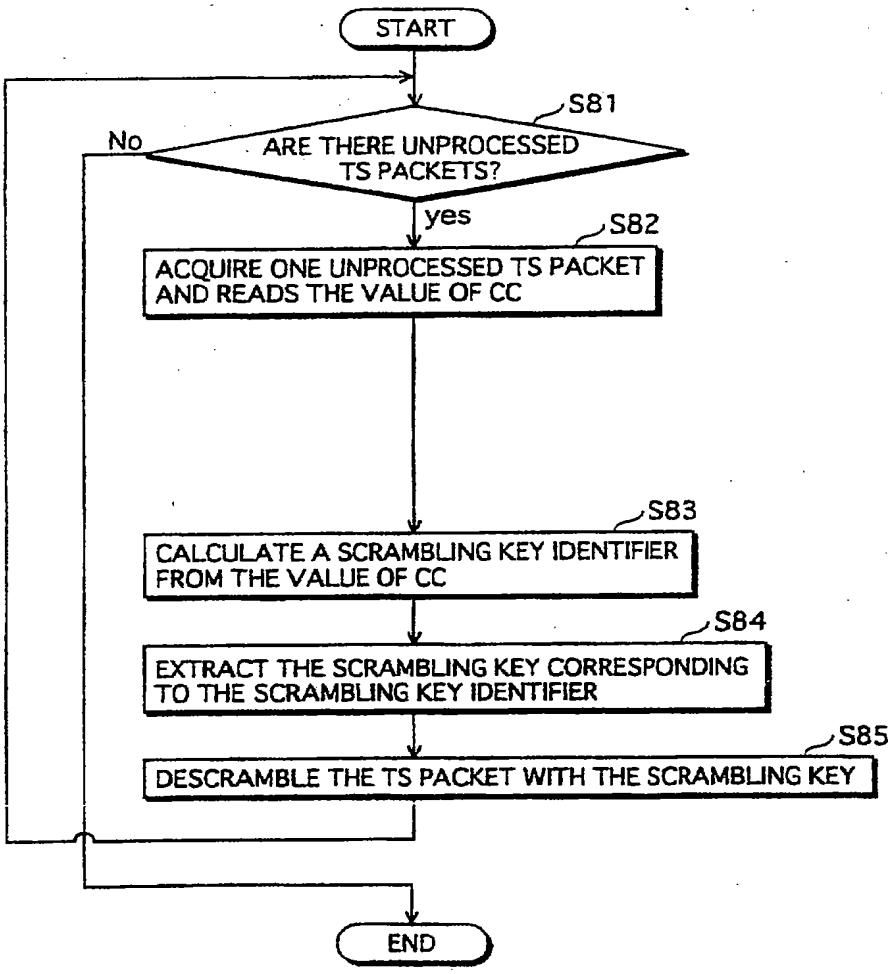

START
S81
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S82
ACQUIRE ONE UNPROCESSED TS PACKET AND READS THE VALUE OF CC
S83
CALCULATE A SCRAMBLING KEY IDENTIFIER FROM THE VALUE OF CC
S84
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE SCRAMBLING KEY IDENTIFIER
S85
DESCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG.27

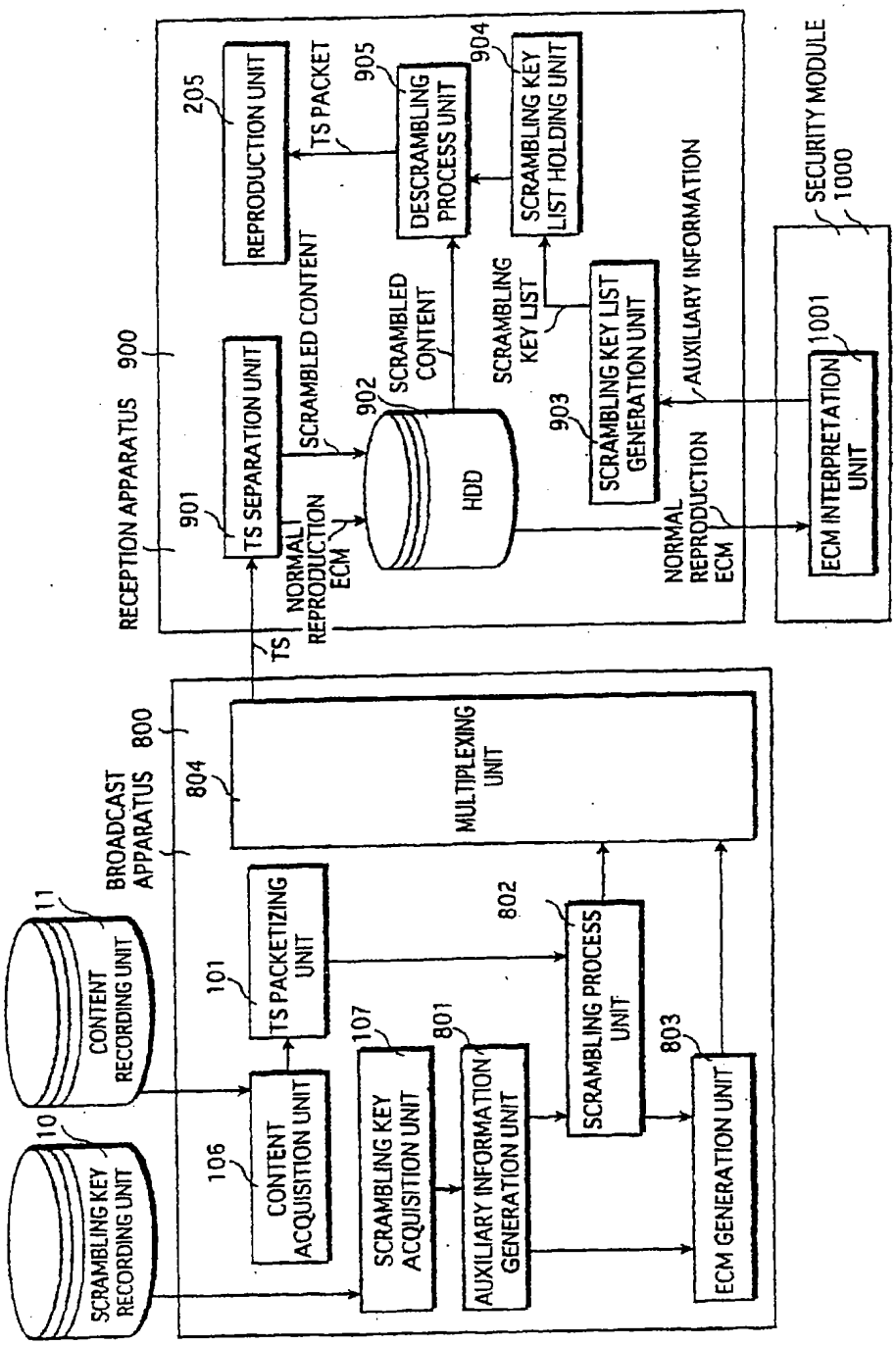

SCRAMBLING KEY RECORDING UNIT
10
CONTENT RECORDING UNIT
11
BROADCAST APPARATUS
800
CONTENT ACQUISITION UNIT
106
TS PACKETIZING UNIT
101
SCRAMBLING KEY ACQUISITION UNIT
107
AUXILIARY INFORMATION GENERATION UNIT
801
SCRAMBLING PROCESS UNIT
802
ECM GENERATION UNIT
803
MULTIPLEXING UNIT
804
TS
NORMAL REPRODUCTION ECM
RECEPTION APPARATUS
900
TS SEPARATION UNIT
901
SCRAMBLED CONTENT
HDD
902
SCRAMBLED CONTENT
SCRAMBLING KEY LIST GENERATION UNIT
903
SCRAMBLING KEY LIST
SCRAMBLING KEY LIST HOLDING UNIT
904
DESCRAMBLING PROCESS UNIT
905
TS PACKET
REPRODUCTION UNIT
205
AUXILIARY INFORMATION
NORMAL REPRODUCTION ECM
SECURITY MODULE
1000
ECM INTERPRETATION UNIT
1001

FIG.28

DATA STRUCTURE OF SCRAMBLING KEY LIST GENERATION DESCRIPTOR

CA_Ks_ListInfo_descriptor() {	
descriptor_tag	1 BYTE
descriptor_length	1 BYTE
Ks_id	1 BYTE
TS_packet_number	2 BYTES
Ks	8 BYTES
}	

Ks_id	:SCRAMBLING KEY IDENTIFIER (TO IDENTIFY SCRAMBLING KEYS)
TS_packet_number	:THE NUMBER OF TS PACKETS SCRAMBLED WITH THE Ks
Ks	:SCRAMBLING KEY

FIG.29

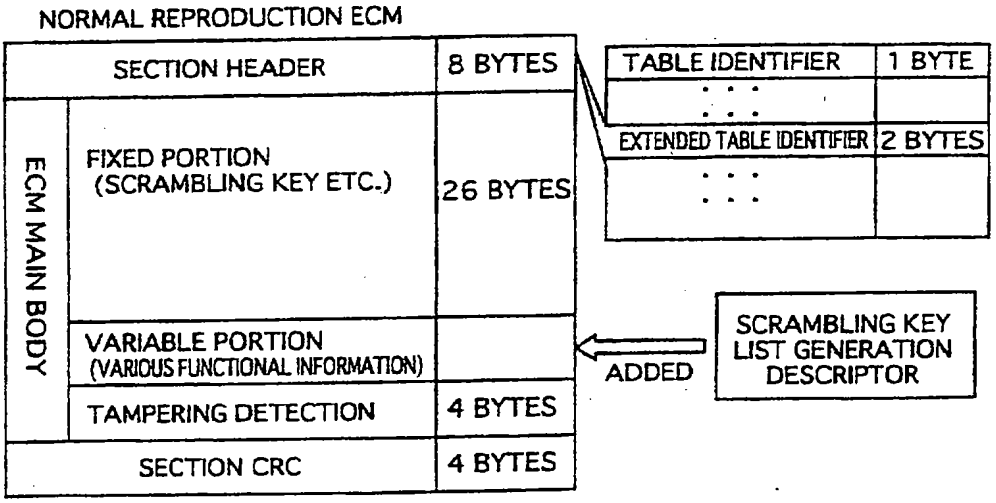

NORMAL REPRODUCTION ECM
SECTION HEADER
8 BYTES
ECM MAIN BODY
FIXED PORTION (SCRAMBLING KEY ETC.)
26 BYTES
VARIABLE PORTION (VARIOUS FUNCTIONAL INFORMATION)
TAMPERING DETECTION
4 BYTES
SECTION CRC
4 BYTES
TABLE IDENTIFIER
1 BYTE
EXTENDED TABLE IDENTIFIER
2 BYTES
ADDED
SCRAMBLING KEY LIST GENERATION DESCRIPTOR

FIG.30

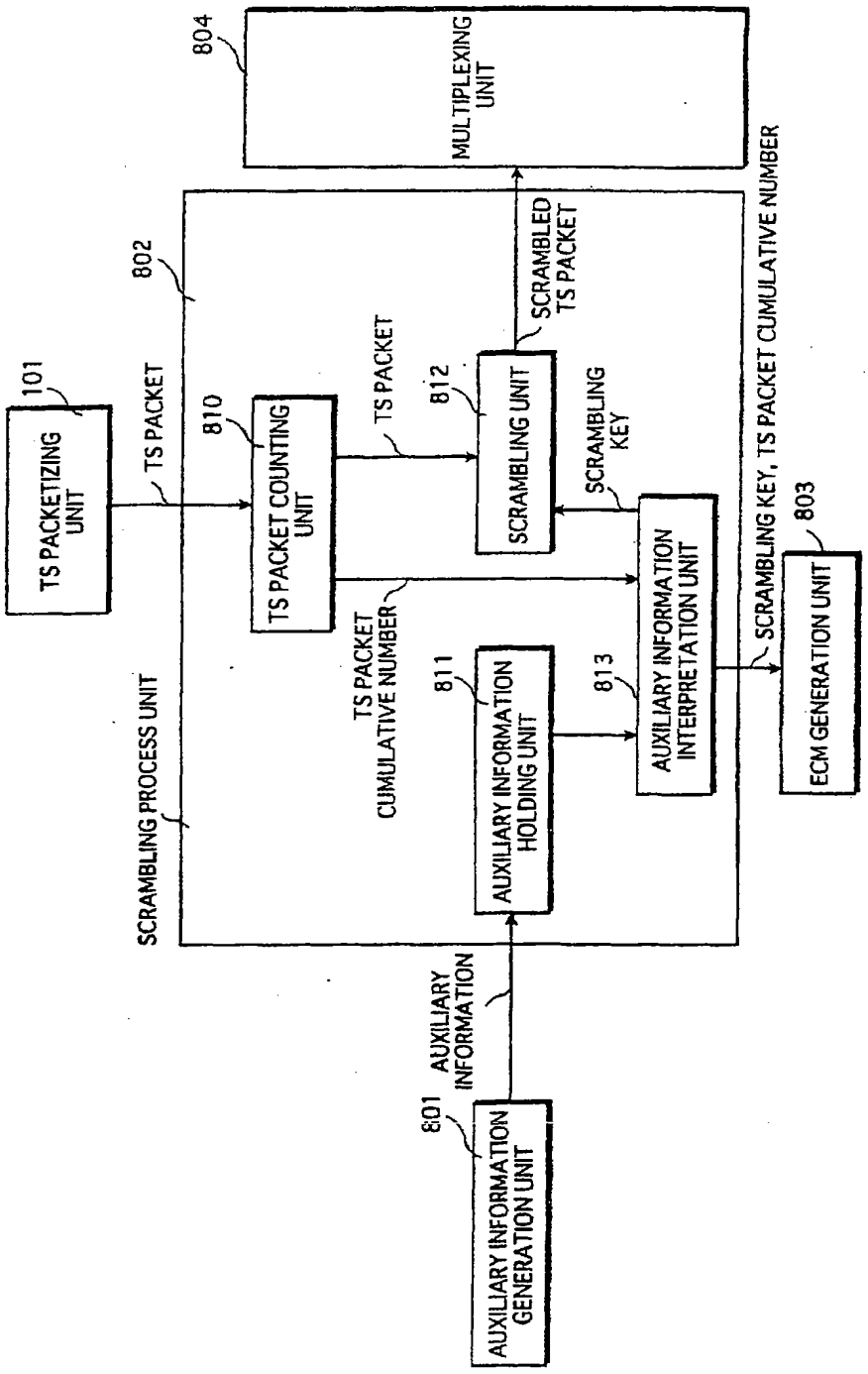

804
MULTIPLEXING UNIT
802
SCRAMBLED TS PACKET
101
TS PACKETIZING UNIT
TS PACKET
810
TS PACKET COUNTING UNIT
TS PACKET
812
SCRAMBLING UNIT
SCRAMBLING KEY
TS PACKET CUMULATIVE NUMBER
811
AUXILIARY INFORMATION HOLDING UNIT
813
AUXILIARY INFORMATION INTERPRETATION UNIT
SCRAMBLING KEY, TS PACKET CUMULATIVE NUMBER
803
ECM GENERATION UNIT
SCRAMBLING PROCESS UNIT
AUXILIARY INFORMATION
801
AUXILIARY INFORMATION GENERATION UNIT

FIG.31

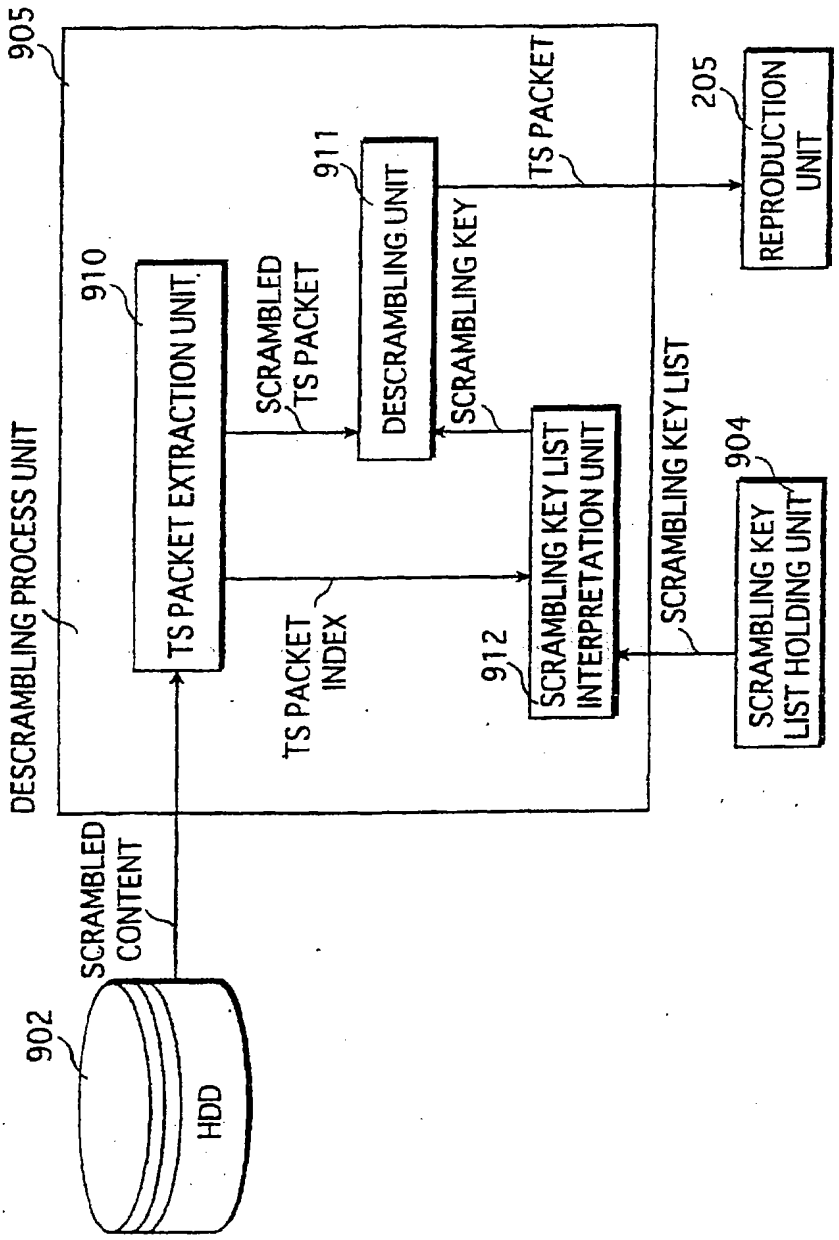

905
DESCRAMBLING PROCESS UNIT
910
TS PACKET EXTRACTION UNIT
911
DESCRAMBLING UNIT
912
SCRAMBLING KEY LIST INTERPRETATION UNIT
904
SCRAMBLING KEY LIST HOLDING UNIT
205
REPRODUCTION UNIT
902
HDD
SCRAMBLED CONTENT
SCRAMBLED TS PACKET
SCRAMBLING KEY
TS PACKET
TS PACKET INDEX
SCRAMBLING KEY LIST

FIG.32

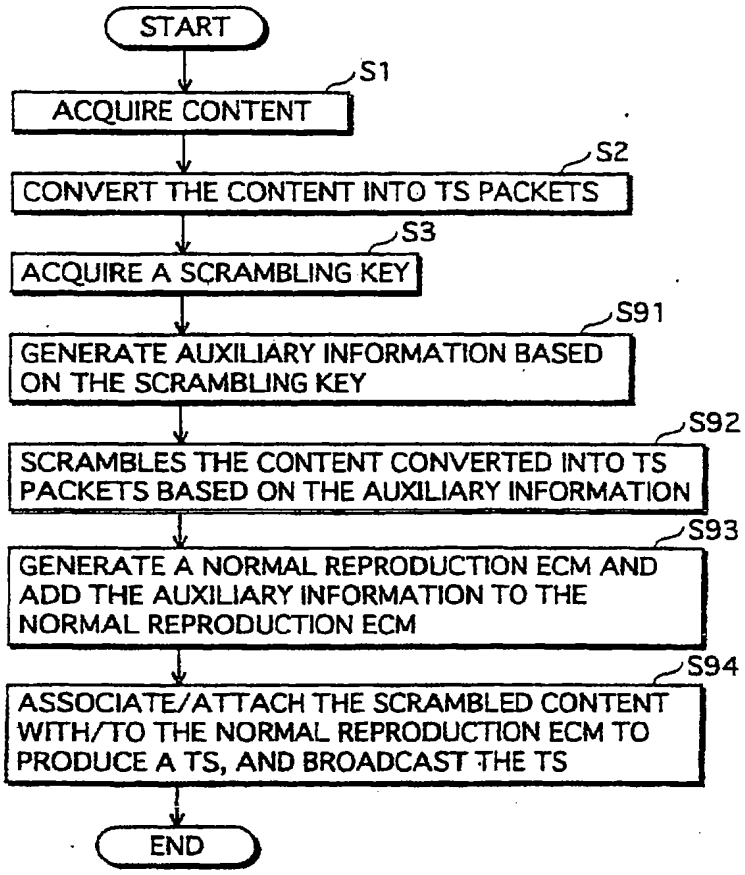

START
S1
ACQUIRE CONTENT
S2
CONVERT THE CONTENT INTO TS PACKETS
S3
ACQUIRE A SCRAMBLING KEY
S91
GENERATE AUXILIARY INFORMATION BASED ON THE SCRAMBLING KEY
S92
SCRAMBLES THE CONTENT CONVERTED INTO TS PACKETS BASED ON THE AUXILIARY INFORMATION
S93
GENERATE A NORMAL REPRODUCTION ECM AND ADD THE AUXILIARY INFORMATION TO THE NORMAL REPRODUCTION ECM
S94
ASSOCIATE/ATTACH THE SCRAMBLED CONTENT WITH/TO THE NORMAL REPRODUCTION ECM TO PRODUCE A TS, AND BROADCAST THE TS
END

FIG.33

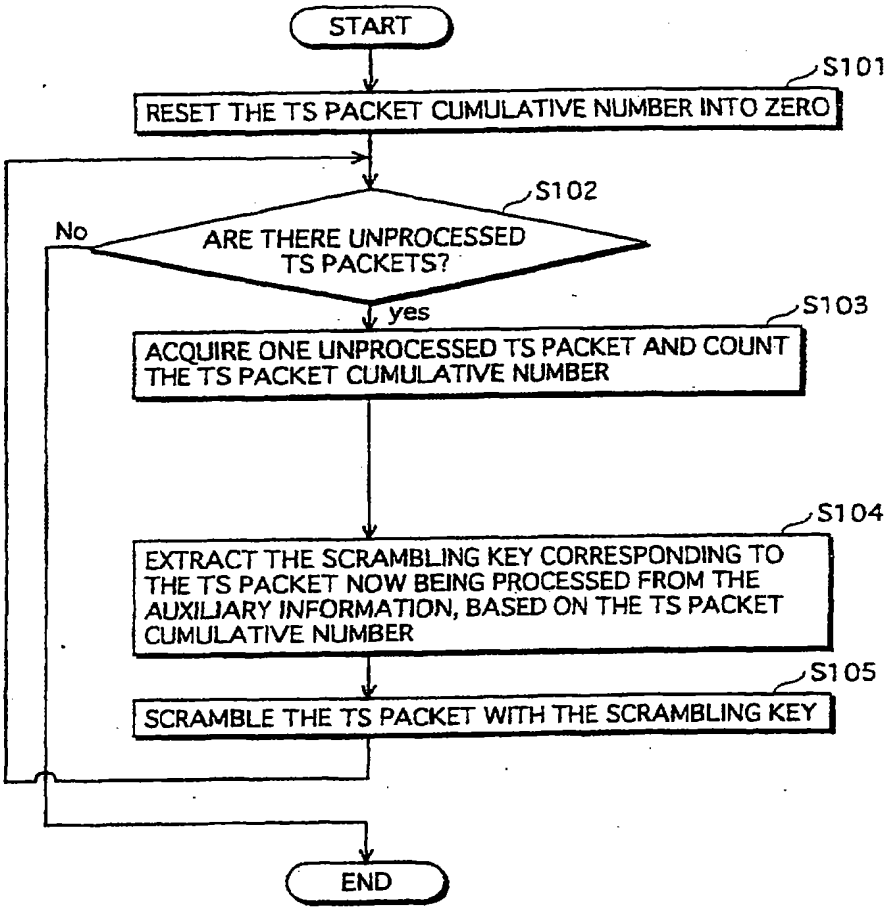

START
S101
RESET THE TS PACKET CUMULATIVE NUMBER INTO ZERO
S102
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S103
ACQUIRE ONE UNPROCESSED TS PACKET AND COUNT THE TS PACKET CUMULATIVE NUMBER
S104
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE TS PACKET NOW BEING PROCESSED FROM THE AUXILIARY INFORMATION, BASED ON THE TS PACKET CUMULATIVE NUMBER
S105
SCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG.34

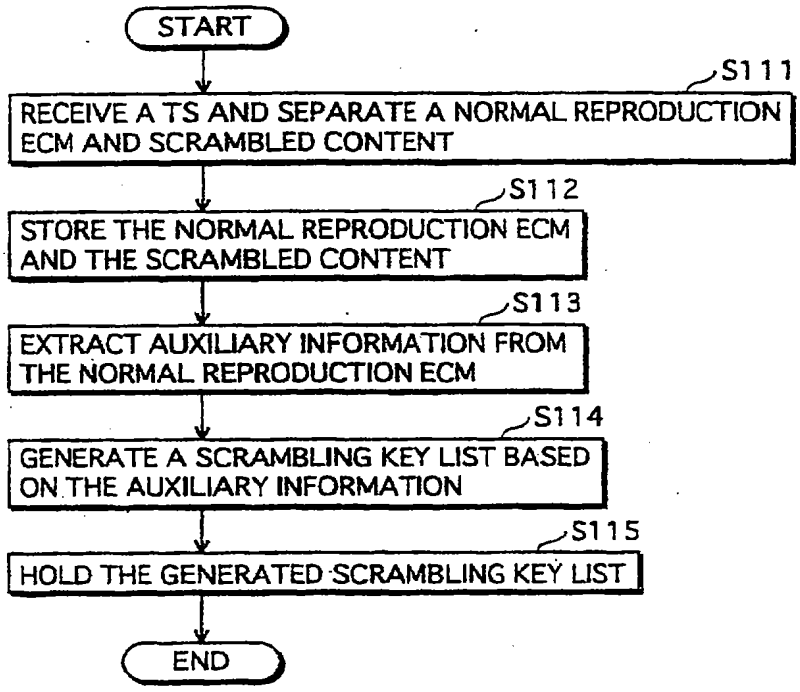

START
S111
RECEIVE A TS AND SEPARATE A NORMAL REPRODUCTION ECM AND SCRAMBLED CONTENT
S112
STORE THE NORMAL REPRODUCTION ECM AND THE SCRAMBLED CONTENT
S113
EXTRACT AUXILIARY INFORMATION FROM THE NORMAL REPRODUCTION ECM
S114
GENERATE A SCRAMBLING KEY LIST BASED ON THE AUXILIARY INFORMATION
S115
HOLD THE GENERATED SCRAMBLING KEY LIST
END

FIG.35

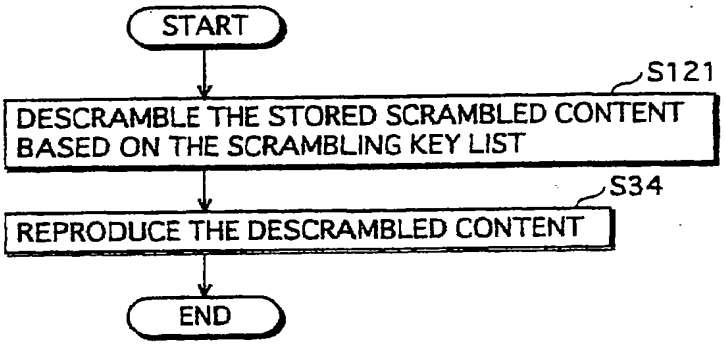

START
S121
DESCRAMBLE THE STORED SCRAMBLED CONTENT BASED ON THE SCRAMBLING KEY LIST
S34
REPRODUCE THE DESCRAMBLED CONTENT
END

FIG.36

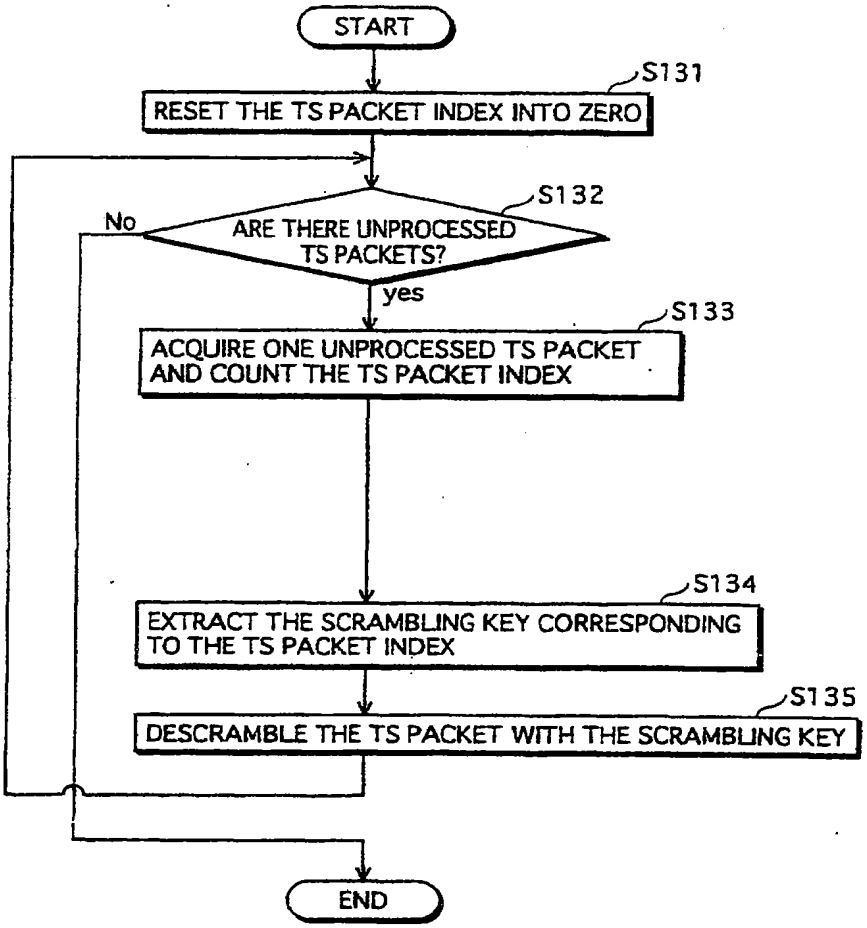

START
S131
RESET THE TS PACKET INDEX INTO ZERO
S132
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S133
ACQUIRE ONE UNPROCESSED TS PACKET AND COUNT THE TS PACKET INDEX
S134
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE TS PACKET INDEX
S135
DESCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG.37

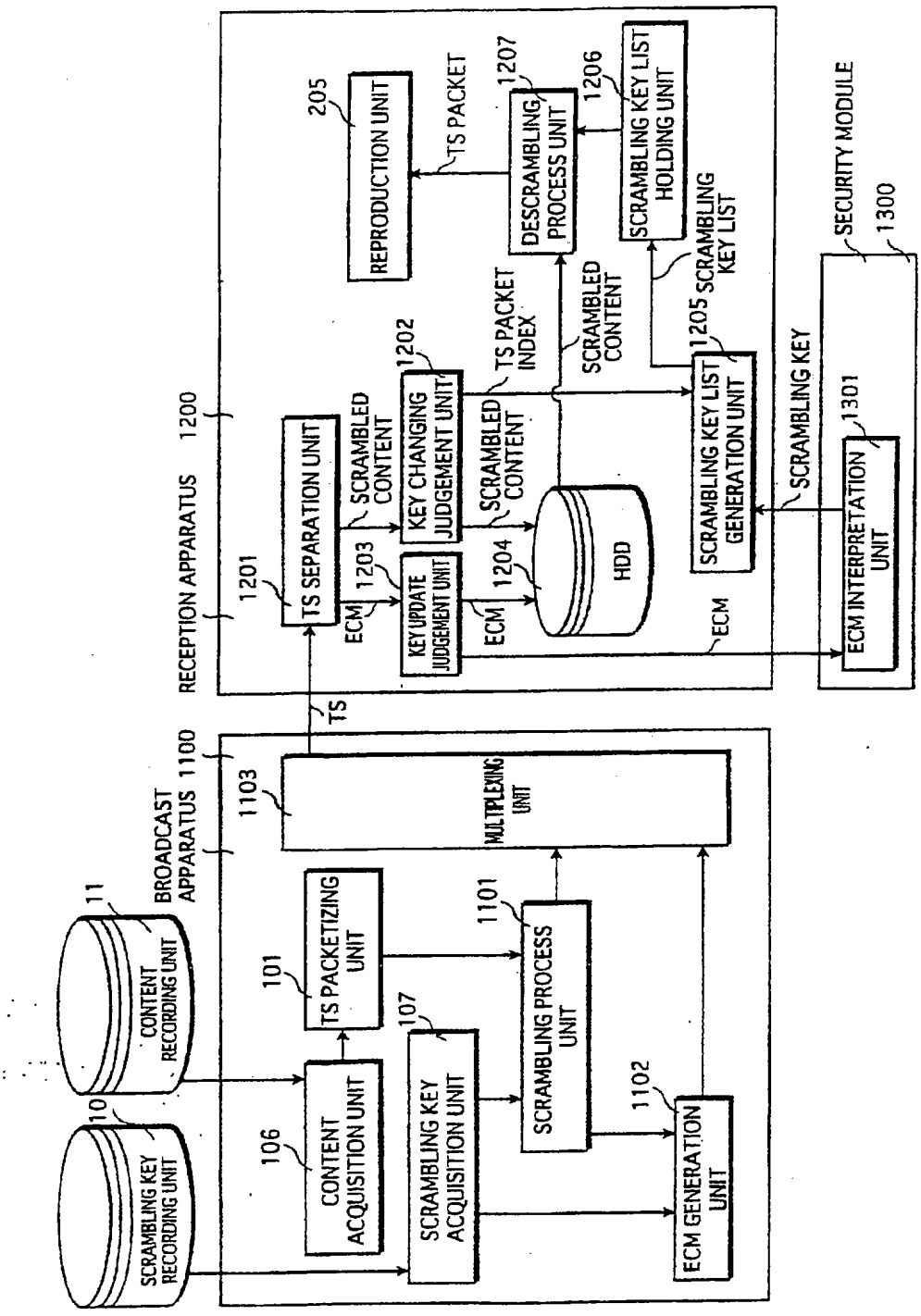

BROADCAST APPARATUS 1100
RECEPTION APPARATUS 1200
SECURITY MODULE 1300
SCRAMBLING KEY RECORDING UNIT
CONTENT RECORDING UNIT
CONTENT ACQUISITION UNIT
TS PACKETIZING UNIT
SCRAMBLING KEY ACQUISITION UNIT
SCRAMBLING PROCESS UNIT
ECM GENERATION UNIT
MULTIPLEXING UNIT
TS
TS SEPARATION UNIT
KEY UPDATE JUDGEMENT UNIT
KEY CHANGING JUDGEMENT UNIT
HDD
SCRAMBLING KEY LIST GENERATION UNIT
DESCRAMBLING PROCESS UNIT
SCRAMBLING KEY LIST HOLDING UNIT
REPRODUCTION UNIT
ECM INTERPRETATION UNIT
SCRAMBLED CONTENT
TS PACKET INDEX
SCRAMBLING KEY LIST
SCRAMBLING KEY
ECM
TS PACKET

FIG.38

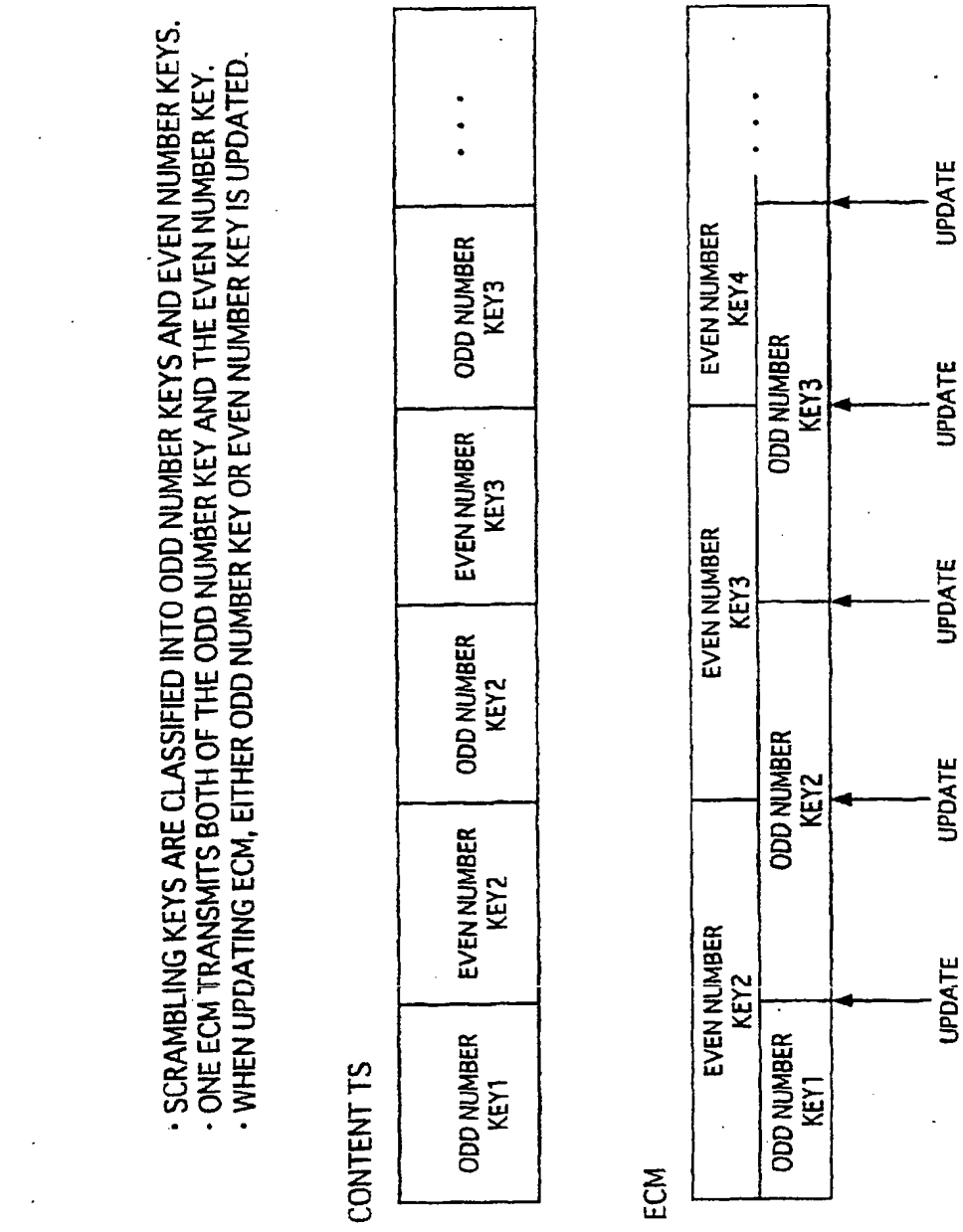
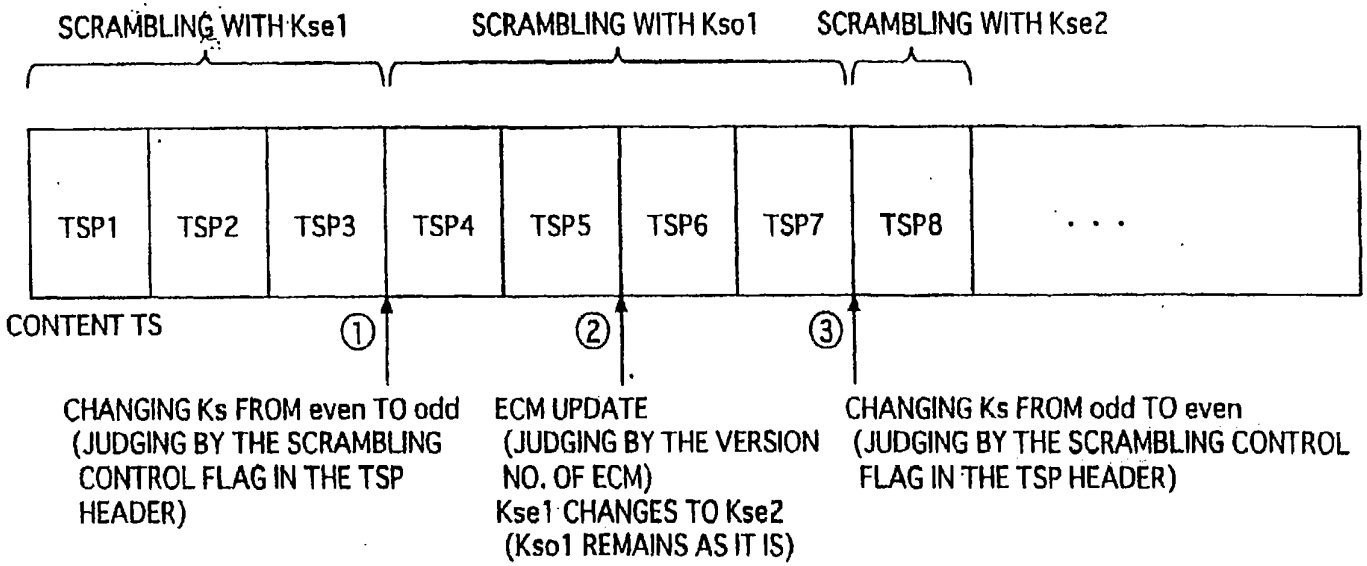

• SCRAMBLING KEYS ARE CLASSIFIED INTO ODD NUMBER KEYS AND EVEN NUMBER KEYS.
• ONE ECM TRANSMITS BOTH OF THE ODD NUMBER KEY AND THE EVEN NUMBER KEY.
• WHEN UPDATING ECM, EITHER ODD NUMBER KEY OR EVEN NUMBER KEY IS UPDATED.
CONTENT TS
ODD NUMBER KEY1
EVEN NUMBER KEY2
ODD NUMBER KEY2
EVEN NUMBER KEY3
ODD NUMBER KEY3
. . .
ECM
EVEN NUMBER KEY2
EVEN NUMBER KEY3
EVEN NUMBER KEY4
ODD NUMBER KEY1
ODD NUMBER KEY2
ODD NUMBER KEY3
. . .
UPDATE
UPDATE
UPDATE
UPDATE
UPDATE

FIG.39



TSP : TS PACKET
Ks : SCRAMBLING KEY
Kse : SCRAMBLING KEY (EVEN NUMBER KEY)
Kso : SCRAMBLING KEY (ODD NUMBER KEY)

SCRAMBLING CONTROL FLAG

SCRAMBLING FLAG VALUE	DESCRIPTION
00	NOT SCRAMBLED
01	NO DEFINITION
10	SCRAMBLED (EVEN NUMBER KEY)
11	SCRAMBLED (ODD NUMBER KEY)

EP 1 215 905 B1

FIG. 40

SCRAMBLING KEY LIST AT THE TIMING OF ① IN FIG. 39

Ks_id	1
TS_packet_number	3
Ks	Kse 1
Ks_id	2
TS_packet_number	
Ks	Kso 1

UNDERLINED INFORMATION IS ADDED.

SCRAMBLING KEY LIST AT THE TIMING OF ③ IN FIG. 39

Ks_id	1
TS_packet_number	3
Ks	Kse 1
Ks_id	2
TS_packet_number	4
Ks	Kso 1
Ks_id	3
TS_packet_number	
Ks	Kse 2

AT THE TIMING OF ② IN FIG. 39, THE SCRAMBLING KEY LIST IS NOT UPDATED, BUT STORED ECM CHANGES AS FOLLOWS.

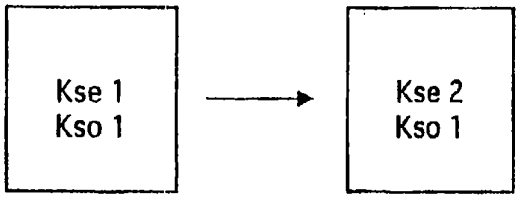


FIG.41

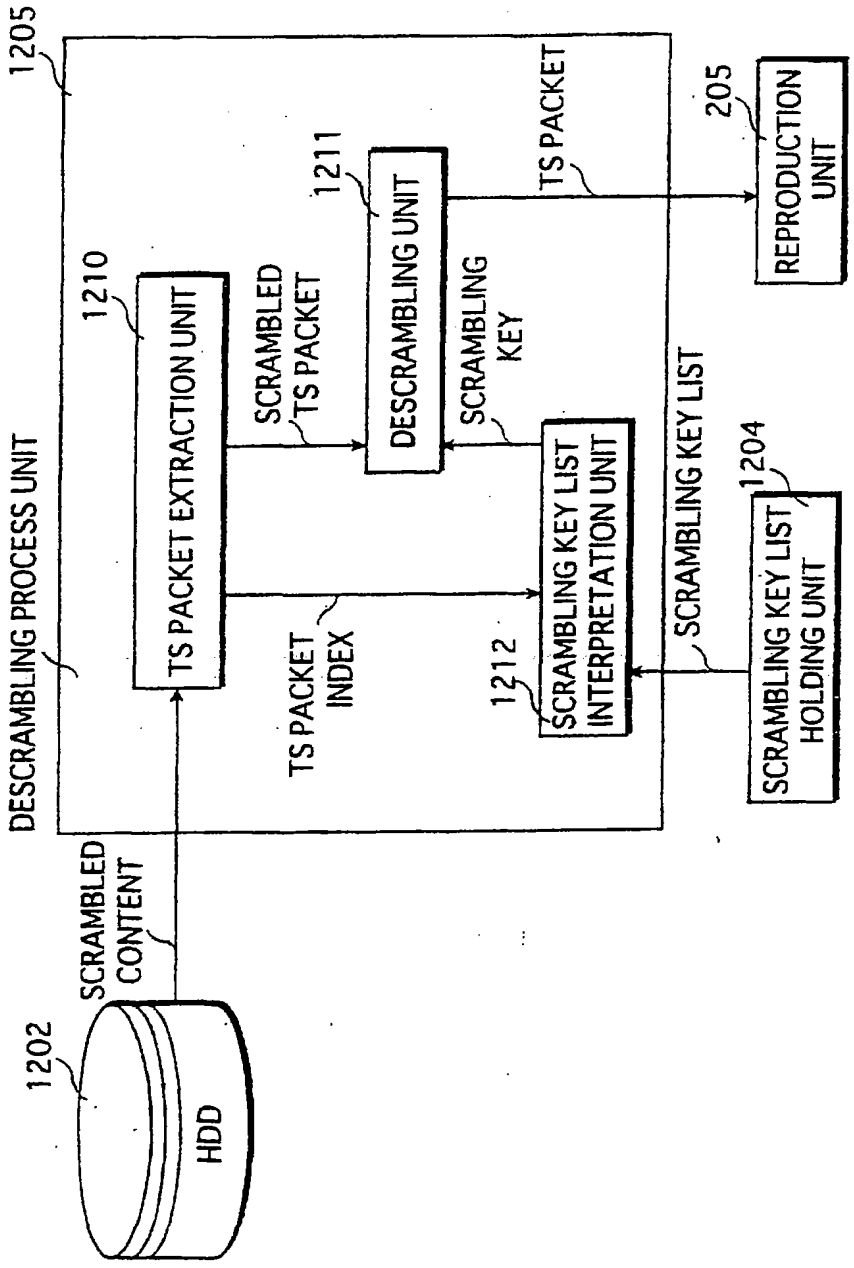

1205
DESCRAMBLING PROCESS UNIT
1210
TS PACKET EXTRACTION UNIT
SCRAMBLED TS PACKET
1211
DESCRAMBLING UNIT
TS PACKET
205
REPRODUCTION UNIT
SCRAMBLING KEY
TS PACKET INDEX
1212
SCRAMBLING KEY LIST INTERPRETATION UNIT
SCRAMBLING KEY LIST
1204
SCRAMBLING KEY LIST HOLDING UNIT
SCRAMBLED CONTENT
1202
HDD

FIG.42

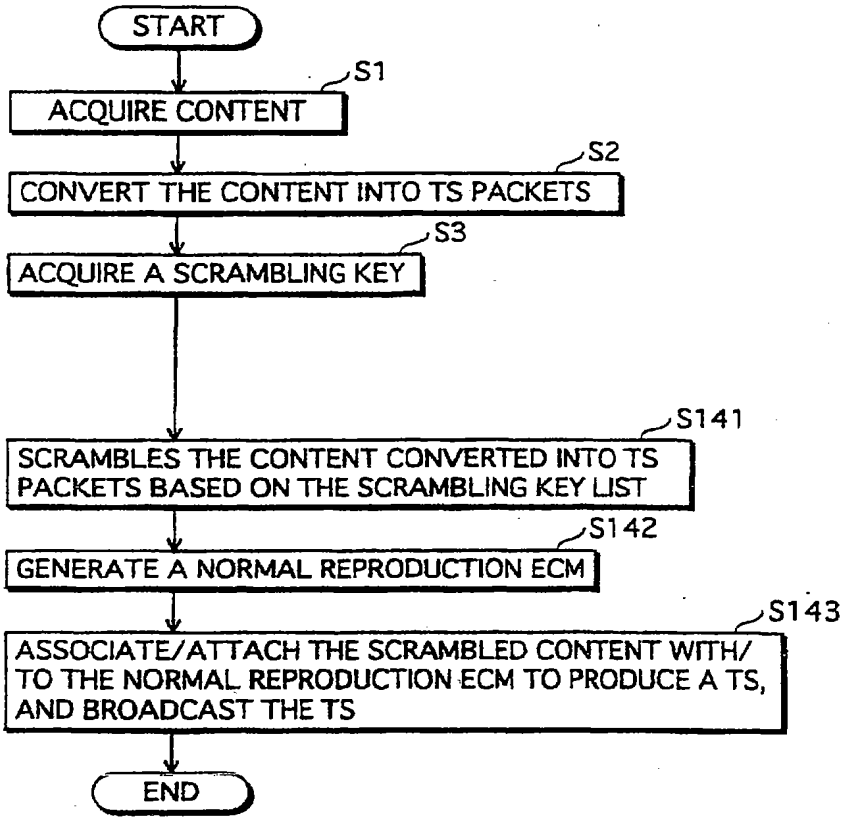

START
S1
ACQUIRE CONTENT
S2
CONVERT THE CONTENT INTO TS PACKETS
S3
ACQUIRE A SCRAMBLING KEY
S141
SCRAMBLES THE CONTENT CONVERTED INTO TS PACKETS BASED ON THE SCRAMBLING KEY LIST
S142
GENERATE A NORMAL REPRODUCTION ECM
S143
ASSOCIATE/ATTACH THE SCRAMBLED CONTENT WITH/ TO THE NORMAL REPRODUCTION ECM TO PRODUCE A TS, AND BROADCAST THE TS
END

FIG.43

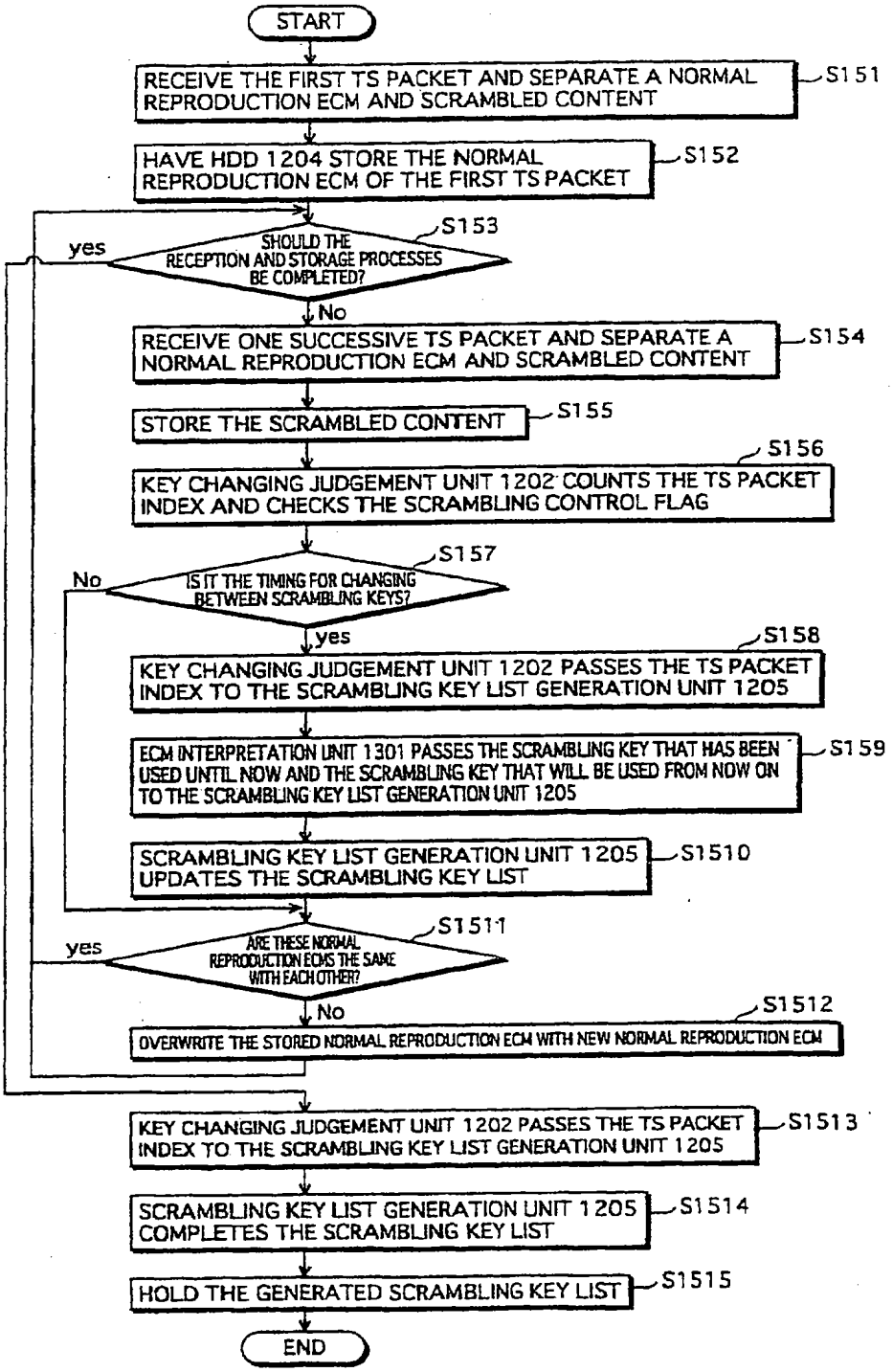

START
RECEIVE THE FIRST TS PACKET AND SEPARATE A NORMAL REPRODUCTION ECM AND SCRAMBLED CONTENT
S151
HAVE HDD 1204 STORE THE NORMAL REPRODUCTION ECM OF THE FIRST TS PACKET
S152
S153
yes
SHOULD THE RECEPTION AND STORAGE PROCESSES BE COMPLETED?
No
RECEIVE ONE SUCCESSIVE TS PACKET AND SEPARATE A NORMAL REPRODUCTION ECM AND SCRAMBLED CONTENT
S154
STORE THE SCRAMBLED CONTENT
S155
S156
KEY CHANGING JUDGEMENT UNIT 1202 COUNTS THE TS PACKET INDEX AND CHECKS THE SCRAMBLING CONTROL FLAG
S157
No
IS IT THE TIMING FOR CHANGING BETWEEN SCRAMBLING KEYS?
yes
S158
KEY CHANGING JUDGEMENT UNIT 1202 PASSES THE TS PACKET INDEX TO THE SCRAMBLING KEY LIST GENERATION UNIT 1205
ECM INTERPRETATION UNIT 1301 PASSES THE SCRAMBLING KEY THAT HAS BEEN USED UNTIL NOW AND THE SCRAMBLING KEY THAT WILL BE USED FROM NOW ON TO THE SCRAMBLING KEY LIST GENERATION UNIT 1205
S159
SCRAMBLING KEY LIST GENERATION UNIT 1205 UPDATES THE SCRAMBLING KEY LIST
S1510
S1511
yes
ARE THESE NORMAL REPRODUCTION ECMS THE SAME WITH EACH OTHER?
No
S1512
OVERWRITE THE STORED NORMAL REPRODUCTION ECM WITH NEW NORMAL REPRODUCTION ECM
KEY CHANGING JUDGEMENT UNIT 1202 PASSES THE TS PACKET INDEX TO THE SCRAMBLING KEY LIST GENERATION UNIT 1205
S1513
SCRAMBLING KEY LIST GENERATION UNIT 1205 COMPLETES THE SCRAMBLING KEY LIST
S1514
HOLD THE GENERATED SCRAMBLING KEY LIST
S1515
END

FIG.44

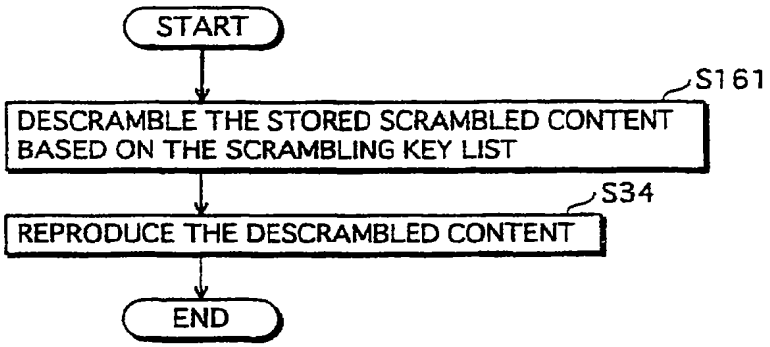

START
S161
DESCRAMBLE THE STORED SCRAMBLED CONTENT BASED ON THE SCRAMBLING KEY LIST
S34
REPRODUCE THE DESCRAMBLED CONTENT
END

FIG.45

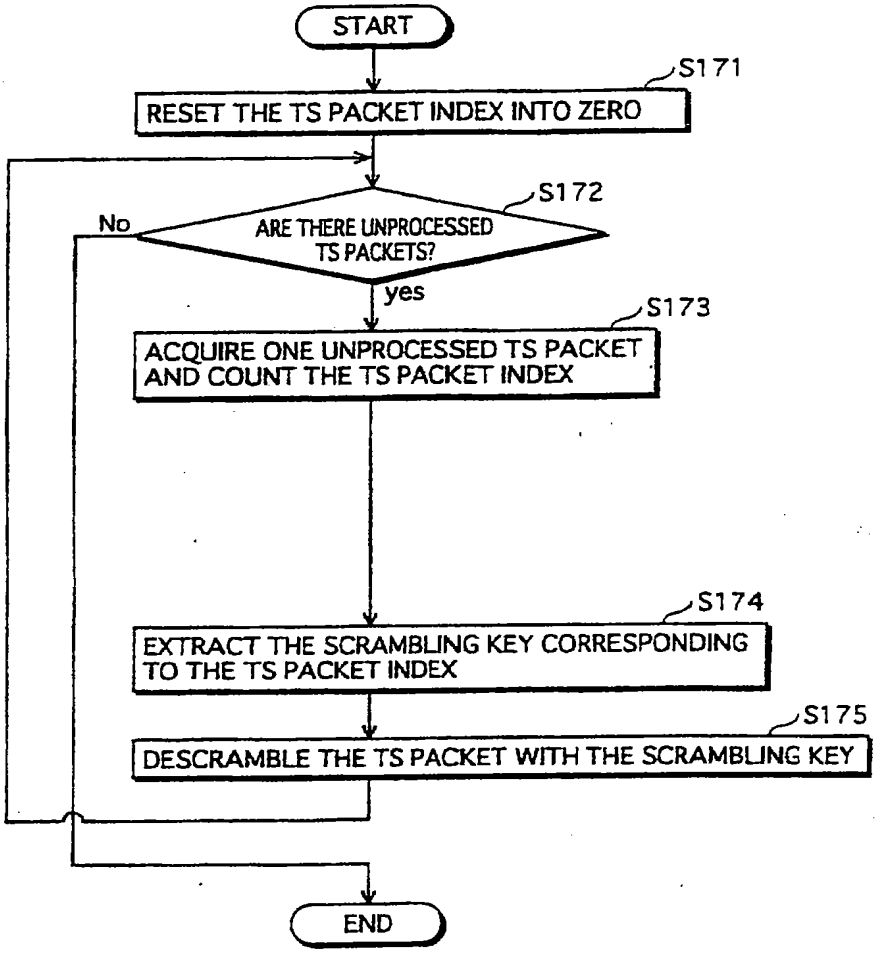

START
S171
RESET THE TS PACKET INDEX INTO ZERO
S172
No
ARE THERE UNPROCESSED TS PACKETS?
yes
S173
ACQUIRE ONE UNPROCESSED TS PACKET AND COUNT THE TS PACKET INDEX
S174
EXTRACT THE SCRAMBLING KEY CORRESPONDING TO THE TS PACKET INDEX
S175
DESCRAMBLE THE TS PACKET WITH THE SCRAMBLING KEY
END

FIG.46

DATA STRUCTURE OF I PICTURE LIST DESCRIPTOR

for(i=0; i <N; i++) {	
Ipic_id	2 BYTES
first_packet_position	2 BYTES
last_packet_position	2 BYTES
}	

Ipic_id : I PICTURE IDENTIFIER (TO IDENTIFY I PICTURES)
first_packet_position : THE FIRST PACKET POSITION OF THE I PICTURE
(THE NUMBER OF TS PACKETS COUNTED FROM THE BEGINNING OF THE FILE)
last_packet_position : THE LAST PACKET POSITION OF THE I PICTURE
(THE NUMBER OF TS PACKETS COUNTED FROM THE BEGINNING OF THE FILE)